

Historical OSINT: OPSEC-Aware Money Mule Recruiters Hire, Host Crimeware and Malvertisements

(2013-01-05 16:10)

In the following intelligence brief, I will perform an analysis of the cybercriminal operations involving a group of

individuals that operated successfully though 2009/2010, recruiting money mules, hosting ZeuS crimeware, and

participating in a malvertising campaign.

Compared to a previous analysis where I profiled the [1]**offensive client-side exploitation campaigns** launched by

money mule recruiters, in this analysis I'll emphasize on yet another OPSEC-aware ([2]**Operational Security**) gang of cybercriminals, this time blocking access to Google and anti-money laundering Web sites/research, in an attempt to

trick the newly recruited mules into thinking that they're working for a legitimate company, preventing them from

obtaining info on their new "employer".

Key summary points:

- The group originally launched its operations in 2009, primary focusing on highly targeted money mule recruitment campaigns
- Only two of the malicious domains involved in the 2009/2010's campaigns are still active, with the first serving

adult content, and the second offering name server services to pharmaceutical scams, indicating they're didn't

quite left the cybercrime ecosystem just yet

- The cybercriminals behind the campaign impersonated the legitimate [3]**Sprott Asset Management** company,

and blocked access to its official site on mule's PCs that executed the malicious SSL Certificate supplied to them

as a requirement for joining the fake company

- Upon execution, the bogus SSL Certificate executable modified the HOSTS file on the affected hosts, blocking

access to [4]**ddanchev.blogspot.com** and to [5]**bobbear.co.uk** to prevent potential money mules from reach-

ing my "[6]**Keeping Money Mule Recruiters on a Short Leash**" series, and bobbear's vast archive of collected intelligence on money mule recruitment campaigns

- The group hosted multiple ZeuS crimeware variants using the same infrastructure as the money mule recruit-

ment campaigns, and also participated in a malvertising campaign

- Although their initial 2009 operations were launched from (**AS39134**), they later on migrated to a Kazakhstan-

based bulletproof hosting provider (**AS50793**) that's no longer in operation, although there's a high probability

that the Kazakhstan hosting service was part of a franchise, and is currently operating in another part of the

world. The Web site of the bulletproof hosting provider was hosted in Ukraine (**AS6714**), an AS also known to

have participated in numerous crimeware campaigns

- The malicious activity (besides their operation) was found for (**AS39134**) indicating that they probably got kicked out of the hosting provider for their attempts to recruit money mules

- The domain name of the Kazakhstan-based bulletproof hosting provider (**AS50793**) was registered using a GMail account in 2010

- The Kazakhstan-based bulletproof ISP's domain name is currently registered to an Iranian citizen, two years

after the malicious activities took place, with no signs of malicious activity currently taking place there

a

5

This post has been reproduced from [7]Dancho Danchev's blog. Follow him [8]on Twitter.

1. <http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html>

2. http://en.wikipedia.org/wiki/Operations_security

3. <http://www.sprott.com/>

4. <http://ddanchev.blogspot.com/>

5. <http://www.bobbear.co.uk/>

6. <https://www.google.com/#hl=en&tbo=d&sclient=psy-ab&q=site:ddanchev.blogspot.com+%22keeping+money+mule%22&o>

[q=site:ddanchev.blogspot.com+%22keeping+money+mule%22&](https://www.google.com/#hl=en&tbo=d&sclient=psy-ab&q=site:ddanchev.blogspot.com+%22keeping+money+mule%22&o)

7. <http://ddanchev.blogspot.com/>

8. <http://twitter.com/danchodanchev>

6



Historical OSINT - Profiling an OPSEC-Unaware Vendor of GSM/USB ATM Skimmers and Pinpads

(2013-01-05 20:42)

On daily basis, I profile over a dozen of newly advertised (verified) vendors of ATM skimmers, indicating that this

market segment is still quite successful, thanks to the overall demand for these 'tools-of-the-trade', allowing potential

cybercriminals to enter the world of ATM skimming.

In this post part of the "Historical OSINT" series, I'll profile the underground market proposition of a vendor

of GSM/USB ATM Skimmers and Pinpads, that appeared on my radar back in 2008, with an emphasis on the lack

of OPSEC (Operational Security) applied by them, and the IP hosting changes of their main domain that took place

throughout 2008, in particular, offer evidence of active multi-tasking on behalf of the same gang of cybercriminals.

What's particularly interesting about this vendor is the fact that, instead of advertising across popular and

well known cybercrime-friendly Web communities, they themselves created a community around the market

proposition, and started pitching their offer across the public Web, a clear indication for a lack of OPSEC (Operational

Security) awareness.

On 2006-04-06, **darkforum.net** (ICQ 16-09-61/160961) was registered using the **alsaleh@gawab.com** email.

On 2009-01-07, the registration email changed to **blanerds@hushmail.com**. These emails are not known to have

been used in previous cybercrime-friendly campaigns.

Throughout 2008, the **darkforum.net** domain constantly changed IPs. The following is a complete list of the

IP changes:

64.74.96.241

69.64.145.229 - IP already profiled in a [1]**previously published analysis**

63.251.92.197



216.8.177.23

69.25.142.57

208.73.212.12

87.242.73.96 - known [2]**C &C server**

64.208.225.139

The advertised brochure of the vendor:

Overview of the technology involved: Here is how it all works.

Full operating instructions are included with the entire package, this page is here for informative purposes. The Card Reader reads ATM & credit cards and sends the data tracks through SMS to a phone. The pin-pad catches the pushing

of the pin number through the keypad and also sends the data through SMS.

SMS data comes to a programmable mobile phone number, which you will set to a safe number of yours. It is

advised to connect your phone to a computer, and download the track data to your computer as it arrives. After

every 2 message track+pin combo, an SMS is sent from each GSM device with a status update. From your computer, you can keep track of the whole operation.

The GSM Kit comes with an MSR206 device and track writing software. From your computer, you retrieve the track data and pin numbers from SMS messages, and then write the tracks to swipe cards with the cloned ATM/Credit cards, you simply use the pin to cash them out at ATM machines.

Receiving:

Received Data on the computer is encrypted. For the decryption, there is a separate program, which is included on

the software DVD. Decrypted data is then ready to be written on cards.

Thus we have a secure working environment. None of your cashiers or crew can get the unencrypted data.

8



Only the user of the software, who controls the operation. This kit is built on brand new technology. We have put a lot of time and money into the development and design. As a result, this is currently the most efficient method of retrieving dumps and pins.

for example the first skimmers were used with a camera, and on the given moment of skimmer it works with

the transmission of data on network GSM, with the sending SMS or with the subtraction of data after calling it. In this

case the complete reliability of the work of equipment, checked by time and experience of many people. For example

now we use the multilayer printed-circuit boards, similar, as are used in the laptop computers or mob telephones,

with the silver contacts and the working from the oxidation although previously they were altogether only old boards.

Now for the size decrease is necessary to proceed with decent expenditures in order to decrease the sizes and in this

case to increase reliability.

Our skimmers were actually originally developed for personal use, not for sale. They were designed with the

most robust, smallest and most efficient parts at each stage of the building process.

Why small? Well, it is better to have a small unit, that fits discretely onto the ATM machine. Why GSM? Because it

is possible to receive SMS at from a remote location. Nobody has ever been caught by police with a GSM skimmer,

to the best of our knowledge. Each day our team is working on the development of newer and newer technologies.

From time to time we apply our improvements to our range of products. Thus we from time to time change to new

designs of housings; we improve the capability of batteries, or the switching system. For example, the new version of

our software has some improvements over previous versions and is regularly updated. Usually clients send on their

feature requests and we are frequently building them into our newest kits.

9



Our skimmers can read a change in the rate of card conduction. For example, if we insert the card slowly, and

then accelerate it, our magnetic strip reader will read and correct this. We read both tracks info from both sides

of the strip. We read reliably, with a 99.9 % correct rate of reading. Sending of SMS occurs from the internal

components of two Sony Ericsson 850i units. The batteries, visible in some of the pictures are from Motorola

phones. The internal circuitry of the phones is connected to a digital circuit and chip which receive the informa-

tion from the pinpad and magnetic reader, respectfully. You will need 3 sim cards, pre-paid is recommended. Each

reading sends 4 SMS messages, 1 with the track information, 1 with the pin, and 1 from each unit with a status update.

On each sim card, you will have to save the phone number of your home mobile phone's sim card under the

name "home". The internal circuitry and interface with the SE850i unit will look to this number to send both the track

data and the pin numbers.

The internal processing chip encrypts the data before sending sms to the computer. In the kit, the decoding

program is included which with one click will transfer the crypted dump into plain text. On opening this program, it is necessary to enter password. But if password is incorrect that program will close with a system error message, rather

than responding with an incorrect password message. This is an obvious security feature. Each unit has an individual

serial number and password. The password is included in the full package. It is possible to request that the password

be communicated online, rather than be included with the software and package.

I will give couple of working examples of scenarios. If someone attempts to open the program and types an incorrect

password, an error message is displayed and the software will "crash". It gives the impression that the software is simply not working. But if the correct password is entered, then it will start. If necessary, it is possible to simply say that the software is just something downloaded from the Internet, but it does not work, and you forgot to remove it.

And no specialist will be able to prove what kind of program it is.

The exterior appearance and feel of our devices is built based on the original appearance of the ATM machine.

In other words, if in one instrument incorporates smooth lines, and sleek curves, then our device will appear very

10



similar on its exterior housing. It is virtually unnoticeable that there has been a modification to the ATM. The paint, with which we spray our housings is matched to the paint on the original ATMs. Our method of colouring accurately

reproduces the originals, while maintaining all the characteristics of colouring, including varying temperature

conditions, the angle of incidence of the paint, pressure, time of polymerization, etc.

As such we attained a perfect match of paint, tone of paint, reflection, and nuances with the different angles

of incidence of light, feeling of the surface and so forth. On the job, this looks and feels exactly the same as an

un-modified ATM. All instruments are powered from Li-on batteries. A charger is included in the complete set. Each

battery is sufficient for 2-3 days of work (at a rated temperature of 22 Celsius). We have carried out extensive tests to find the maximum quantity of SMS which can be sent from one battery. Tests showed that we could send 1400 SMS

from one battery without a recharge. The majority of the time, the instrument stands in standby mode. Very little

power is used until the card is inserted or the pinpad is pressed, when track data is collected, and pins are

collected.

The complete set comes with everything you need to run a full operation. However, the batteries need to be

fully charged and recharged. This means that it is necessary to give 2-3 complete cycles of charging and discharging.

This makes possible for battery to work longer. As a rule by this "warming-up" of the batteries an increase of the length of time they will operate will increase by 30-40 %.

Again we stress that we are moving ahead, and developing more advanced devices. The current range for sale has

been extensively tested and proven as a reliable kit.

USB Flash memory skimmers:

We have a cheaper range of non-GSM skimming kit for sale. This is mostly bought by new users, as experienced,

wealthy crews will be using the more modern GSM skimmers.

Our range starts with a basic skimmer & hidden camera, pre installed inside a discrete case, with flash storage

and timestamps. Our basic skimmers are just as discrete and physically sound as our expensive GSM kit. They contain

a 512 mb flash card, and a ROM chip with tiny card writer to record the info to the micro sd card. These kits come

with an MSR206 and a multi card reader to retrieve the dumps + pins from both devices.



If you already own an MSR206, it can be removed from the package and a small discount can be given.

Pinpad info

Basic features of our pinpads are:

- 1. Ultra thin, around 3mm and it looks slimmer because of some design tricks*
- 2. Real Stainless-Steel Material Frame and the keys*
- 3. Exact same size as the actual ATM's pinpad*
- 4. Special plated Frame and Keys that does not hold any Fingerprints well*
- 5. Ultra low power consumption*
- 6. Various languages supported*



Technical Information on Charging and Communicating:

As usual, you may charge your pinpad through the USB communication cable. Charging is automatic, when you plug the cable into the pinpad, it will start charging. You can communicate with the pinpad while charging. You should

charge your pinpad for a minimum 2 hours before operation. Try to use a USB Port on a Desktop Computer instead of

a Laptop or USB hub. If u need to use a laptop then make sure you are using laptop with its power adapter connected,

otherwise you will try to charge pinpads Battery with laptop's battery and this will result in poor charging. Remember, you have to check date and time of your pinpad and adjust it if needed before operation. Setting the date/time is very easy using the software provided.

There are some limits on USB Charging. USB Charging is good if your skimming operation last 12-16 hours. If

you require your pinpad to last longer then you have to buy Lithium-Polymer(Li-Po) 3.7v Generic charger for charging

the battery of your pinpad. We can include this with the full kit for an extra cost. You may contact to us if you bought a Li-Po charger and want to use it with your pinpad.

You must be extremely careful when plugging the cable into the pinpad! There was not enough space in the

pinpad for us to place a generic USB socket that eliminates user mistakes when plugging in the cable. We used plain

socket that allows user to plug cable in any direction/position. If you plug the cable in the wrong direction/position then your pinpad electronics may be damaged. There also a risk to your battery. So pay special attention when

plugging the cable into your pinpad for data transfer and/or charging. Check the picture below for concise instructions

on how to plug the cable into your pinpad.

Follow these steps for easy plugging:

- 1. Identify the Red Wire on the cable's socket*
- 2. Identify the Red Wire on pinpads Socket*
- 3. Red wire of pinpads socket should always be near the Crystal, and should join with the other red wire.*

13



- 4. Then plug it like this:*

Information on Installing and Removing to/from ATM:

*You should use transparent fast glues for glue your Pinpad.
You have to be very careful on NOT TO GLUE the*

*Membrane of your Pinpad. You only need to glue the back of
the frame of the Pinpad, only places where it touches*

*the ATM. Again, no membrane or keys!!! You should use 2
holes designed for removing Pinpad from the ATM. You*

may use a small screwdriver or knife or similar.

*You have to be very careful when removing the pinpad from
the ATM. You should not damage membrane of*

*the pinpad when using screwdriver or knife to remove it.
Several practice attempts, on a flat surface are recom-
mended.*

You should try with very small amount of glue for your tests to see and understand how it sticks. Then you

should decide what amount of glue will be used when you are on the job. Your tests are the key to your success. Test

your skimmer on the ATM with no Glue/Less Glue etc. for experience. Never start to skimming before feeling you

understand all the logic.

Our Software Description

To work with a skimmer, a computer is necessary of course. You need to save your dumps (card data tracks) there! We

will provide you with software, which can completely control your skimmer. Using this software, you can download

dumps from skimmer/input them from SMS, remove them from skimmer unit, etc.

The program saves everything in crypted form. So that you don't have to worry about being ripped off. No

one will be able to retrieve your data without the password. The password is included in the complete package, or can

be sent separately online for security purposes. Each skimmer is basically a small computer, with a processor, flash

14



storage, the internals of a SE850i mobile(cellular/GSM) phone, through which it sends info, and it has an EEPROM

chip which boots up and operates the unit. So that takes care of software and passwords. Software is supplied in the complete set with the equipment directly to the buyer, even if transaction is done through some mediator, and passwords are given only to the buyer. We make so that the mediator cannot obtain both the software and the passwords.

The program does not show dumps on the screen. Also it does not preserve dumps in the open form. With the retention they are ciphered by a serious key. At the start of program it will request your password. But if password is introduced incorrect that it simply closes down and prints a system error on the screen. This creates the impression that the program is simply nonworking. And if you will not input the correct password, there's no way to even know what kind of program it is. This was created so that non-critical people with an attempt at the start would not attempt to select password. Let's just say suddenly, the police get the laptop, on which the program is installed. Naturally, they will ask you about the password. If you are creative, you will give them a fake password, which they enter it, and the program will simply shut down and writes that an error occurred. This will give the impression that the program is nonworking. And you can boldly tell that the "program never worked, and I just forgot to delete it".

The dumps are stored in an encrypted file, which it is not possible to decrypt. There will be no evidence left on your computer, once the police do not get a hold of the password.

The software itself is easy to use. There is no extra options or excess instructions. It is self explanatory, but

full instructions are included with the full kit. If you have any other questions we will try our best to answer them

from our administration team or our software developers.

15



Safety:

We are often asked questions about safety when we are working with skimmers. On this page, I will try to give some

good safety advice for cashing out and operating a successful skimming operation.

Observation:

It is recommended to observe the target ATM, unobtrusively for 1-2 days before hand. Record at what times the ATM is

busy, what times it is quiet, and at what time it is serviced and money is put into the machine, if it is a free standing unit.

Equipment preparation:

It is recommended to check all your equipment before the installation. Make sure that you have practised with some dummy ATM cards before hand and have transferred your own ATM card, or similar into track data, SMS, decrypt, and write to a "white card" with your MSR206 card writer.

16



Work for the fitter/installer:

The installer must be good with their hands. They must accurately and rapidly carry out his work, and quietly leave the area. Some crews will have their fitter dress up in a uniform to make them appear to be servicing the ATM. This is not such a good idea. Just go to the ATM when it is quiet. Perhaps have an assistant stand a distance away, to distract passers-by or other users of the ATM. The whole process can take less than 30 seconds.

Operation of the device:

Place, and the time of the installation should be selected beforehand. An observation point might be necessary.

There should be somewhere to safely park your car from which to observe the operation of the skimmer and pinpad.

If you are waiting in a car, it is not recommended that you have a laptop + msr + phone receiving and writing the

data. If the operation is busted in this manner, you lose everything. However, if you are at home, you will have at

least several hours in which to write the cards and cash them out. Your observation person should have enough food,

water, etc to last in the car for the complete duration of the operation if possible. One plan that some crews use now is observation from an apartment or hotel close to the ATM. With this, you can cut down on the number of your crew.

But be careful use fake identification if you can.

Full details of the installation are described with pictures in a series of PDF files included on the software and

instructions DVD. The fitter/installer should put a card into the machine and reject it quickly when fitting. The receiver, working on the "home" computer, will receive the track, and confirm that it stuck on properly. 99 % of the time, it sticks no problem. This is also useful to find that the card is ejecting properly.

17



When removing equipment, your crew should be trained and ready. Some crews do not risk withdrawing equipment

as the average 1-day run will net \$20,000- \$50,000 USD depending on where you are. However if you are confident

about removing it, you should take it to run the operation again. If apprehended while removing the equipment, the

remover should protest innocence. They should say that they saw something suspicious, and were trying to take it

off the ATM to being to police/bank. The crew member should look and act like a respectable citizen. You do not

need a crew of thugs for this operation. You need a well-spoken, relaxed, confident team. It can be done with just 2

people, but 3 is recommended. Observing the guy removing the kit is a good idea, and walkie-talkies are useful. If

the observer sees someone approaching the removal guy, he should "squak" his walkie-talkie, and the remover can disappear quickly.

18



Cashing out the money:

On many ATMs, there is a monitoring camera. Cameras are usually motion activated. We advise that you do not stay

at one ATM more than 5 minutes, and do not tie up an ATM if there are people in the queue. Do not always cash out

at an ATM belonging to one single bank, nor should you ever cash out your cards on the ATM that you skimmed them

on.

19



Many crews will have several people working on cashing out, and they work 10 cards per person per time, all

returning the money to the controller periodically. If you are cashing out at night at a quiet ATM, having hoods up is a good idea to prevent the camera from seeing you. That's just about everything you need to know to operate a safe, extremely lucrative ATM skimming business.

20



The Kit includes a software dvd (with full instructions), MSR206, Skimmer + Pinpad, and encryption key to decode

dumps which are encrypted on the devices. Note: Only skimmed tracks are encrypted, pins are not encrypted.
Rental

Schemes are available, where we keep the encryption key for the 1st operation of the skimmer, and provide you with

20 unencrypted dumps + pins. This rental scheme costs €1400 for USB kits, and €2200 for GSM kits.

My initial discovery of this cybercrime-friendly market proposition, coincides with the publication of a related

post back in 2008, for the first time ever publicly disclosing important details regarding the emergence of [3]**ATM**

Skimmers with built-in GSM modules.

Nowadays, these are everyday reality.

This post has been reproduced from [4]Dancho Danchev's blog. Follow him [5]on Twitter.

1. <http://ddanchev.blogspot.com/2008/08/facebook-malware-campaigns-rotating.html>
2. <http://www.bothunter.net/live/2011-10-15/index.html>
3. <http://www.zdnet.com/blog/security/scammers-introduce-atm-skimmers-with-built-in-sms-notification/2000>
4. <http://ddanchev.blogspot.com/>
5. <http://twitter.com/danchodanchev>

21



Historical OSINT - Profiling an OPSEC-Unaware Vendor of GSM/USB ATM Skimmers and Pinpads

(2013-01-05 20:42)

On daily basis, I profile over a dozen of newly advertised (verified) vendors of ATM skimmers, indicating that this

market segment is still quite successful, thanks to the overall demand for these 'tools-of-the-trade', allowing potential

cybercriminals to enter the world of ATM skimming.

In this post part of the "Historical OSINT" series, I'll profile the underground market proposition of a vendor

of GSM/USB ATM Skimmers and Pinpads, that appeared on my radar back in 2008, with an emphasis on the lack

of OPSEC (Operational Security) applied by them, and the IP hosting changes of their main domain that took place

throughout 2008, in particular, offer evidence of active multi-tasking on behalf of the same gang of cybercriminals.

What's particularly interesting about this vendor is the fact that, instead of advertising across popular and

well known cybercrime-friendly Web communities, they themselves created a community around the market

proposition, and started pitching their offer across the public Web, a clear indication for a lack of OPSEC (Operational

Security) awareness.

On 2006-04-06, **darkforum.net** (ICQ 16-09-61/160961) was registered using the **alsaleh@gawab.com** email.

On 2009-01-07, the registration email changed to **blanerds@hushmail.com**. These emails are not known to have

been used in previous cybercrime-friendly campaigns.

Throughout 2008, the **darkforum.net** domain constantly changed IPs. The following is a complete list of the

IP changes:

64.74.96.241

69.64.145.229 - IP already profiled in a [1]**previously published analysis**

63.251.92.197

22



216.8.177.23

69.25.142.57

208.73.212.12

87.242.73.96 - known [2]**C &C server**

64.208.225.139

The advertised brochure of the vendor:

Overview of the technology involved: Here is how it all works.

Full operating instructions are included with the entire package, this page is here for informative purposes. The Card Reader reads ATM & credit cards and sends the data tracks through SMS to a phone. The pin-pad catches the pushing

of the pin number through the keypad and also sends the data through SMS.

SMS data comes to a programmable mobile phone number, which you will set to a safe number of yours. It is

advised to connect your phone to a computer, and download the track data to your computer as it arrives. After

every 2 message track+pin combo, an SMS is sent from each GSM device with a status update. From your computer,

you can keep track of the whole operation.

The GSM Kit comes with an MSR206 device and track writing software. From your computer, you retrieve the track

data and pin numbers from SMS messages, and then write the tracks to swipe cards with the cloned ATM/Credit

cards, you simply use the pin to cash them out at ATM machines.

Receiving:

Received Data on the computer is encrypted. For the decryption, there is a separate program, which is included on

the software DVD. Decrypted data is then ready to be written on cards.

Thus we have a secure working environment. None of your cashiers or crew can get the unencrypted data.

23



Only the user of the software, who controls the operation. This kit is built on brand new technology. We have put

a lot of time and money into the development and design. As a result, this is currently the most efficient method of retrieving dumps and pins.

for example the first skimmers were used with a camera, and on the given moment of skimmer it works with

the transmission of data on network GSM, with the sending SMS or with the subtraction of data after calling it. In this case the complete reliability of the work of equipment, checked by time and experience of many people. For example

now we use the multilayer printed-circuit boards, similar, as are used in the laptop computers or mob telephones,

with the silver contacts and the working from the oxidation although previously they were altogether only old boards.

Now for the size decrease is necessary to proceed with decent expenditures in order to decrease the sizes and in this

case to increase reliability.

Our skimmers were actually originally developed for personal use, not for sale. They were designed with the

most robust, smallest and most efficient parts at each stage of the building process.

Why small? Well, it is better to have a small unit, that fits discretely onto the ATM machine. Why GSM? Because it

is possible to receive SMS at from a remote location. Nobody has ever been caught by police with a GSM skimmer,

to the best of our knowledge. Each day our team is working on the development of newer and newer technologies.

From time to time we apply our improvements to our range of products. Thus we from time to time change to new

designs of housings; we improve the capability of batteries, or the switching system. For example, the new version of

our software has some improvements over previous versions and is regularly updated. Usually clients send on their

feature requests and we are frequently building them into our newest kits.

24



Our skimmers can read a change in the rate of card conduction. For example, if we insert the card slowly, and

then accelerate it, our magnetic strip reader will read and correct this. We read both tracks info from both sides

of the strip. We read reliably, with a 99.9 % correct rate of reading. Sending of SMS occurs from the internal

components of two Sony Ericsson 850i units. The batteries, visible in some of the pictures are from Motorola

phones. The internal circuitry of the phones is connected to a digital circuit and chip which receive the informa-

tion from the pinpad and magnetic reader, respectfully. You will need 3 sim cards, pre-paid is recommended. Each

reading sends 4 SMS messages, 1 with the track information, 1 with the pin, and 1 from each unit with a status update.

On each sim card, you will have to save the phone number of your home mobile phone's sim card under the

name "home". The internal circuitry and interface with the SE850i unit will look to this number to send both the track data and the pin numbers.

The internal processing chip encrypts the data before sending sms to the computer. In the kit, the decoding

program is included which with one click will transfer the crypted dump into plain text. On opening this program, it is necessary to enter password. But if password is incorrect that program will close with a system error message, rather

than responding with an incorrect password message. This is an obvious security feature. Each unit has an individual

serial number and password. The password is included in the full package. It is possible to request that the password

be communicated online, rather than be included with the software and package.

I will give couple of working examples of scenarios. If someone attempts to open the program and types an incorrect

password, an error message is displayed and the software will "crash". It gives the impression that the software is simply not working. But if the correct password is entered, then it will start. If necessary, it is possible to simply say that the software is just something downloaded from the Internet, but it does not work, and you forgot to remove it.

And no specialist will be able to prove what kind of program it is.

The exterior appearance and feel of our devices is built based on the original appearance of the ATM machine.

In other words, if in one instrument incorporates smooth lines, and sleek curves, then our device will appear very

25



similar on its exterior housing. It is virtually unnoticeable that there has been a modification to the ATM. The paint, with which we spray our housings is matched to the paint on the original ATMs. Our method of colouring accurately

reproduces the originals, while maintaining all the characteristics of colouring, including varying temperature

conditions, the angle of incidence of the paint, pressure, time of polymerization, etc.

As such we attained a perfect match of paint, tone of paint, reflection, and nuances with the different angles

of incidence of light, feeling of the surface and so forth. On the job, this looks and feels exactly the same as an

un-modified ATM. All instruments are powered from Li-on batteries. A charger is included in the complete set. Each

battery is sufficient for 2-3 days of work (at a rated temperature of 22 Celsius). We have carried out extensive tests to find the maximum quantity of SMS which can be sent from one battery. Tests showed that we could send 1400 SMS

from one battery without a recharge. The majority of the time, the instrument stands in standby mode. Very little

power is used until the card is inserted or the pinpad is pressed, when track data is collected, and pins are

collected.

The complete set comes with everything you need to run a full operation. However, the batteries need to be

fully charged and recharged. This means that it is necessary to give 2-3 complete cycles of charging and discharging.

This makes possible for battery to work longer. As a rule by this "warming-up" of the batteries an increase of the length of time they will operate will increase by 30-40 %.

Again we stress that we are moving ahead, and developing more advanced devices. The current range for sale has

been extensively tested and proven as a reliable kit.

USB Flash memory skimmers:

We have a cheaper range of non-GSM skimming kit for sale. This is mostly bought by new users, as experienced,

wealthy crews will be using the more modern GSM skimmers.

Our range starts with a basic skimmer & hidden camera, pre installed inside a discrete case, with flash storage

and timestamps. Our basic skimmers are just as discrete and physically sound as our expensive GSM kit. They contain

a 512 mb flash card, and a ROM chip with tiny card writer to record the info to the micro sd card. These kits come

with an MSR206 and a multi card reader to retrieve the dumps + pins from both devices.



If you already own an MSR206, it can be removed from the package and a small discount can be given.

Pinpad info

Basic features of our pinpads are:

- 1. Ultra thin, around 3mm and it looks slimmer because of some design tricks*
- 2. Real Stainless-Steel Material Frame and the keys*
- 3. Exact same size as the actual ATM's pinpad*
- 4. Special plated Frame and Keys that does not hold any Fingerprints well*
- 5. Ultra low power consumption*
- 6. Various languages supported*



Technical Information on Charging and Communicating:

As usual, you may charge your pinpad through the USB communication cable. Charging is automatic, when you plug the cable into the pinpad, it will start charging. You can communicate with the pinpad while charging. You should

charge your pinpad for a minimum 2 hours before operation. Try to use a USB Port on a Desktop Computer instead of

a Laptop or USB hub. If u need to use a laptop then make sure you are using laptop with its power adapter connected,

otherwise you will try to charge pinpads Battery with laptop's battery and this will result in poor charging. Remember, you have to check date and time of your pinpad and adjust it if needed before operation. Setting the date/time is very easy using the software provided.

There are some limits on USB Charging. USB Charging is good if your skimming operation last 12-16 hours. If

you require your pinpad to last longer then you have to buy Lithium-Polymer(Li-Po) 3.7v Generic charger for charging

the battery of your pinpad. We can include this with the full kit for an extra cost. You may contact to us if you bought a Li-Po charger and want to use it with your pinpad.

You must be extremely careful when plugging the cable into the pinpad! There was not enough space in the

pinpad for us to place a generic USB socket that eliminates user mistakes when plugging in the cable. We used plain

socket that allows user to plug cable in any direction/position. If you plug the cable in the wrong direction/position then your pinpad electronics may be damaged. There also a risk to your battery. So pay special attention when

plugging the cable into your pinpad for data transfer and/or charging. Check the picture below for concise instructions

on how to plug the cable into your pinpad.

Follow these steps for easy plugging:

- 1. Identify the Red Wire on the cable's socket*
- 2. Identify the Red Wire on pinpads Socket*
- 3. Red wire of pinpads socket should always be near the Crystal, and should join with the other red wire.*

28



- 4. Then plug it like this:*

Information on Installing and Removing to/from ATM:

*You should use transparent fast glues for glue your Pinpad.
You have to be very careful on NOT TO GLUE the*

*Membrane of your Pinpad. You only need to glue the back of
the frame of the Pinpad, only places where it touches*

*the ATM. Again, no membrane or keys!!! You should use 2
holes designed for removing Pinpad from the ATM. You*

may use a small screwdriver or knife or similar.

*You have to be very careful when removing the pinpad from
the ATM. You should not damage membrane of*

*the pinpad when using screwdriver or knife to remove it.
Several practice attempts, on a flat surface are recom-
mended.*

You should try with very small amount of glue for your tests to see and understand how it sticks. Then you

should decide what amount of glue will be used when you are on the job. Your tests are the key to your success. Test

your skimmer on the ATM with no Glue/Less Glue etc. for experience. Never start to skimming before feeling you

understand all the logic.

Our Software Description

To work with a skimmer, a computer is necessary of course. You need to save your dumps (card data tracks) there! We

will provide you with software, which can completely control your skimmer. Using this software, you can download

dumps from skimmer/input them from SMS, remove them from skimmer unit, etc.

The program saves everything in crypted form. So that you don't have to worry about being ripped off. No

one will be able to retrieve your data without the password. The password is included in the complete package, or can

be sent separately online for security purposes. Each skimmer is basically a small computer, with a processor, flash

29



storage, the internals of a SE850i mobile(cellular/GSM) phone, through which it sends info, and it has an EEPROM

chip which boots up and operates the unit. So that takes care of software and passwords. Software is supplied in the complete set with the equipment directly to the buyer, even if transaction is done through some mediator, and passwords are given only to the buyer. We make so that the mediator cannot obtain both the software and the passwords.

The program does not show dumps on the screen. Also it does not preserve dumps in the open form. With the retention they are ciphered by a serious key. At the start of program it will request your password. But if password is introduced incorrect that it simply closes down and prints a system error on the screen. This creates the impression that the program is simply nonworking. And if you will not input the correct password, there's no way to even know what kind of program it is. This was created so that non-critical people with an attempt at the start would not attempt to select password. Let's just say suddenly, the police get the laptop, on which the program is installed. Naturally, they will ask you about the password. If you are creative, you will give them a fake password, which they enter it, and the program will simply shut down and writes that an error occurred. This will give the impression that the program is nonworking. And you can boldly tell that the "program never worked, and I just forgot to delete it".

The dumps are stored in an encrypted file, which it is not possible to decrypt. There will be no evidence left on your computer, once the police do not get a hold of the password.

The software itself is easy to use. There is no extra options or excess instructions. It is self explanatory, but

full instructions are included with the full kit. If you have any other questions we will try our best to answer them

from our administration team or our software developers.

30



Safety:

We are often asked questions about safety when we are working with skimmers. On this page, I will try to give some

good safety advice for cashing out and operating a successful skimming operation.

Observation:

It is recommended to observe the target ATM, unobtrusively for 1-2 days before hand. Record at what times the ATM is

busy, what times it is quiet, and at what time it is serviced and money is put into the machine, if it is a free standing unit.

Equipment preparation:

It is recommended to check all your equipment before the installation. Make sure that you have practised with some dummy ATM cards before hand and have transferred your own ATM card, or similar into track data, SMS, decrypt, and write to a "white card" with your MSR206 card writer.

31



Work for the fitter/installer:

The installer must be good with their hands. They must accurately and rapidly carry out his work, and quietly leave the area. Some crews will have their fitter dress up in a uniform to make them appear to be servicing the ATM. This is not such a good idea. Just go to the ATM when it is quiet. Perhaps have an assistant stand a distance away, to distract passers-by or other users of the ATM. The whole process can take less than 30 seconds.

Operation of the device:

Place, and the time of the installation should be selected beforehand. An observation point might be necessary.

There should be somewhere to safely park your car from which to observe the operation of the skimmer and pinpad.

If you are waiting in a car, it is not recommended that you have a laptop + msr + phone receiving and writing the

data. If the operation is busted in this manner, you lose everything. However, if you are at home, you will have at

least several hours in which to write the cards and cash them out. Your observation person should have enough food,

water, etc to last in the car for the complete duration of the operation if possible. One plan that some crews use now is observation from an apartment or hotel close to the ATM. With this, you can cut down on the number of your crew.

But be careful use fake identification if you can.

Full details of the installation are described with pictures in a series of PDF files included on the software and

instructions DVD. The fitter/installer should put a card into the machine and reject it quickly when fitting. The receiver, working on the "home" computer, will receive the track, and confirm that it stuck on properly. 99 % of the time, it sticks no problem. This is also useful to find that the card is ejecting properly.

32



When removing equipment, your crew should be trained and ready. Some crews do not risk withdrawing equipment

as the average 1-day run will net \$20,000- \$50,000 USD depending on where you are. However if you are confident

about removing it, you should take it to run the operation again. If apprehended while removing the equipment, the

remover should protest innocence. They should say that they saw something suspicious, and were trying to take it

off the ATM to being to police/bank. The crew member should look and act like a respectable citizen. You do not

need a crew of thugs for this operation. You need a well-spoken, relaxed, confident team. It can be done with just 2

people, but 3 is recommended. Observing the guy removing the kit is a good idea, and walkie-talkies are useful. If

the observer sees someone approaching the removal guy, he should "squak" his walkie-talkie, and the remover can disappear quickly.

33



Cashing out the money:

On many ATMs, there is a monitoring camera. Cameras are usually motion activated. We advise that you do not stay

at one ATM more than 5 minutes, and do not tie up an ATM if there are people in the queue. Do not always cash out

at an ATM belonging to one single bank, nor should you ever cash out your cards on the ATM that you skimmed them

on.

34



Many crews will have several people working on cashing out, and they work 10 cards per person per time, all

returning the money to the controller periodically. If you are cashing out at night at a quiet ATM, having hoods up is a good idea to prevent the camera from seeing you. That's just about everything you need to know to operate a safe, extremely lucrative ATM skimming business.

35



The Kit includes a software dvd (with full instructions), MSR206, Skimmer + Pinpad, and encryption key to decode

dumps which are encrypted on the devices. Note: Only skimmed tracks are encrypted, pins are not encrypted.
Rental

Schemes are available, where we keep the encryption key for the 1st operation of the skimmer, and provide you with

20 unencrypted dumps + pins. This rental scheme costs €1400 for USB kits, and €2200 for GSM kits.

My initial discovery of this cybercrime-friendly market proposition, coincides with the publication of a related

post back in 2008, for the first time ever publicly disclosing important details regarding the emergence of [3]**ATM**

Skimmers with built-in GSM modules.

Nowadays, these are everyday reality.

Updates will be posted as soon as new developments take place.

1. <http://ddanchev.blogspot.com/2008/08/facebook-malware-campaigns-rotating.html>
2. <http://www.bothunter.net/live/2011-10-15/index.html>
3. <http://www.zdnet.com/blog/security/scammers-introduce-atm-skimmers-with-built-in-sms-notification/2000>

36

Raw Historical OSINT - Keeping Money Mule Recruiters on a Short Leash - Part Twelve (2013-01-07 22:56)

In the following (historical) intelligence brief, I'll provide you with some raw domain data of fake companies that are known to have attempted to recruit money mules over the past 2 years.

The domains listed here were registered by the same gang of cybercriminals that I've been extensively profil-

ing in previous "Keeping Money Mule Recruiters on a Short Leash" posts.

Money mule recruitment domains:

compassllc-usa.com

linkllc-uk.com

very-compllc.com

click-n-art.com

infotechgroup-inc.com

amplitude-groupmain.tw

magnet-groupinc.cc

allston-groupsec.cc

DEVELOP-INC.COM

MERCYGROUPNET.NET

MERCY-INC.COM

SOLARISGROUPINC.COM

SOLARISGROUPNET.NET

JVC-INC.COM

JVCGROUPNET.NET

EVOLVINGSYSINC.NET

ATCANETWORKS.NET

ATCA-INC.COM

GALLEOGROUPNET.NET

GALLEO-INC.COM

EVOLVINGSYSINC.NET

EVOLVING-INC.COM

NETMARKET-INC.COM

NETMARKETTECH.NET

INFOTECH-GROUPCO.NET

INFOTECH-GROUPINC.COM

INFOTECHGROUP-INC.COM

BANDS-GROUPSVC.COM

BANDS-INC.COM

BANDSGROUP-INC.NET

BANDSGROUPNET.CC

ICT-GROUPCO.COM

ICT-GROUPSVC.NET

ICTGROUPINC.COM

ICTGROUPNET.CC

GIANT-GROUPCO.NET

GIANT-GROUPINC.COM

GIANT-GROUPNET.CC

GIANTGROUPINC.COM

IMPERIAL-GROUPINC.COM

IMPERIAL-GROUPSVC.NET

37

IMPERIALGROUPCO.COM

HOSTGROUP-INC.COM

HOSTGROUPINC.COM

HOSTGROUPNET.CC

HOST-GROUPSVC.NET

CNLGROUP-INC.CC

CNLGROUPNET.NET

CNL-GROUPSVC.COM

CNL-INC.COM

bands-groupsvc.com

bands-inc.com

bandsgroup-inc.net

bandsgroupnet.cc

cnl-groupsvc.com

cnl-inc.com

cnlgroup-inc.cc

cnlgroupnet.net

giant-groupco.net

giant-groupinc.com

giant-groupnet.cc

giantgroupinc.com

host-groupsvc.net

hostgroup-inc.com

hostgroupinc.com

hostgroupnet.cc

ict-groupco.com

ict-groupsvc.net

ictgroupinc.com

ictgroupnet.cc

imperial-groupinc.com

imperial-groupsvc.net

imperialgroupco.com

infotech-groupco.net

infotech-groupinc.com

infotechgroup-inc.com

itcom-groupco.net

itcom-groupfine.cc

itcom-groupsvc.com

itcomgroup-inc.com

mgm-groupsvc.com

mgmgroup-inc.net

mgmgroupinc.com

mgmgrouppnet.cc

usi-groupinc.net

usigroup-inc.com

usigroupinc.com

usigroupnet.cc

NOVARIS-GROUPLLC.TW

NOVARISGROUPMAIN.TW

NOVARIS-GROUPORG.CC

38

VITAL-GROUPCO.CC

VITAL-GROUPCO.TW

VITAL-GROUPINC.TW

PERSEUS-GROUPFINE.TW

PERSEUS-GROUPINC.TW

PERSEUSGROUPLLC.CC

Consider going through my previous research into one of the most popular 'risk-forwarding' tactic used by cy-

bercriminals, namely, money mule recruitment.

Related posts on money mule recruitment:

[1]Keeping Money Mule Recruiters on a Short Leash - Part Eleven

[2]Keeping Money Mule Recruiters on a Short Leash - Part Ten

[3]Keeping Money Mule Recruiters on a Short Leash - Part Nine

[4]Keeping Money Mule Recruiters on a Short Leash - Part Eight - Historical OSINT

[5]Keeping Money Mule Recruiters on a Short Leash - Part Seven

[6]Keeping Money Mule Recruiters on a Short Leash - Part Six

[7]Keeping Money Mule Recruiters on a Short Leash - Part Five

[8]The DNS Infrastructure of the Money Mule Recruitment Ecosystem

[9]Keeping Money Mule Recruiters on a Short Leash - Part Four

[10]Money Mule Recruitment Campaign Serving Client-Side Exploits

[11]Keeping Money Mule Recruiters on a Short Leash - Part Three

[12]Money Mule Recruiters on Yahoo!'s Web Hosting

[13]Dissecting an Ongoing Money Mule Recruitment Campaign

[14]Keeping Money Mule Recruiters on a Short Leash - Part Two

[15]Keeping Reshipping Mule Recruiters on a Short Leash

[16]Keeping Money Mule Recruiters on a Short Leash

[17]Standardizing the Money Mule Recruitment Process

[18]Inside a Money Laundering Group's Spamming Operations

[19]Money Mule Recruiters use ASProx's Fast Fluxing Services

[20]Money Mules Syndicate Actively Recruiting Since 2002

This post has been reproduced from [21]Dancho Danchev's blog.

1. <http://ddanchev.blogspot.com/2011/08/keeping-money-mule-recruiters-on-short.html>

2. <http://ddanchev.blogspot.com/2011/07/keeping-money-mule-recruiters-on-short.html>

3. http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short_30.html

4. http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short_25.html

5. <http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short.html>

6. <http://ddanchev.blogspot.com/2011/03/keeping-money-mule-recruiters-on-short.html>

7. <http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html>

8. <http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html>
9. <http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html>
10. <http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html>
11. <http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html>
12. <http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html>
13. <http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html>
14. <http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html>
15. <http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html>
16. <http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html>

39

17. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>
18. <http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html>
19. <http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asprox-fast.html>

20. <http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html>

21. <http://ddanchev.blogspot.com/>

40

Raw Historical OSINT - Keeping Money Mule Recruiters on a Short Leash - Part Twelve (2013-01-07 22:56)

In the following (historical) intelligence brief, I'll provide you with some raw domain data of fake companies that are

known to have attempted to recruit money mules over the past 2 years.

The domains listed here were registered by the same gang of cybercriminals that I've been extensively profil-

ing in previous "Keeping Money Mule Recruiters on a Short Leash" posts.

Money mule recruitment domains:

compassllc-usa.com

linkllc-uk.com

very-compllc.com

click-n-art.com

infotechgroup-inc.com

amplitude-groupmain.tw

magnet-groupinc.cc

allston-groupsec.cc

DEVELOP-INC.COM

MERCYGROUPNET.NET

MERCY-INC.COM

SOLARISGROUPINC.COM

SOLARISGROUPNET.NET

JVC-INC.COM

JVCGROUPNET.NET

EVOLVINGSYSINC.NET

ATCANETWORKS.NET

ATCA-INC.COM

GALLEOGROUPNET.NET

GALLEO-INC.COM

EVOLVINGSYSINC.NET

EVOLVING-INC.COM

NETMARKET-INC.COM

NETMARKETTECH.NET

INFOTECH-GROUPCO.NET

INFOTECH-GROUPINC.COM

INFOTECHGROUP-INC.COM

BANDS-GROUPSVC.COM

BANDS-INC.COM

BANDSGROUP-INC.NET

BANDSGROUPNET.CC

ICT-GROUPCO.COM

ICT-GROUPSVC.NET

ICTGROUPINC.COM

ICTGROUPNET.CC

GIANT-GROUPCO.NET

GIANT-GROUPINC.COM

GIANT-GROUPNET.CC

GIANTGROUPINC.COM

IMPERIAL-GROUPINC.COM

IMPERIAL-GROUPSVC.NET

41

IMPERIALGROUPCO.COM

HOSTGROUP-INC.COM

HOSTGROUPINC.COM

HOSTGROUPNET.CC

HOST-GROUPSVC.NET

CNLGROUP-INC.CC

CNLGROUPNET.NET

CNL-GROUPSVC.COM

CNL-INC.COM

bands-groupsvc.com

bands-inc.com

bandsgroup-inc.net

bandsgroupnet.cc

cnl-groupsvc.com

cnl-inc.com

cnlgroup-inc.cc

cnlgroupnet.net

giant-groupco.net

giant-groupinc.com

giant-groupnet.cc

giantgroupinc.com

host-groupsvc.net

hostgroup-inc.com

hostgroupinc.com

hostgroupnet.cc

ict-groupco.com

ict-groupsvc.net

ictgroupinc.com

ictgroupnet.cc

imperial-groupinc.com

imperial-groupsvc.net

imperialgroupco.com

infotech-groupco.net

infotech-groupinc.com

infotechgroup-inc.com

itcom-groupco.net

itcom-groupfine.cc

itcom-groupsvc.com

itcomgroup-inc.com

mgm-groupsvc.com

mgmgroup-inc.net

mgmgroupinc.com

mgmgroupnet.cc

usi-groupinc.net

usigroup-inc.com

usigroupinc.com

usigroupnet.cc

NOVARIS-GROUPLLC.TW

NOVARISGROUPMAIN.TW

NOVARIS-GROUPORG.CC

42

VITAL-GROUPCO.CC

VITAL-GROUPCO.TW

VITAL-GROUPINC.TW

PERSEUS-GROUPFINE.TW

PERSEUS-GROUPINC.TW

PERSEUSGROUPLLC.CC

Consider going through my previous research into one of the most popular 'risk-forwarding' tactic used by cy-

bercriminals, namely, money mule recruitment.

Related posts on money mule recruitment:

[1]Keeping Money Mule Recruiters on a Short Leash - Part Eleven

[2]Keeping Money Mule Recruiters on a Short Leash - Part Ten

[3]Keeping Money Mule Recruiters on a Short Leash - Part Nine

[4]Keeping Money Mule Recruiters on a Short Leash - Part Eight - Historical OSINT

[5]Keeping Money Mule Recruiters on a Short Leash - Part Seven

[6]Keeping Money Mule Recruiters on a Short Leash - Part Six

[7]Keeping Money Mule Recruiters on a Short Leash - Part Five

[8]The DNS Infrastructure of the Money Mule Recruitment Ecosystem

[9]Keeping Money Mule Recruiters on a Short Leash - Part Four

[10]Money Mule Recruitment Campaign Serving Client-Side Exploits

[11]Keeping Money Mule Recruiters on a Short Leash - Part Three

[12]Money Mule Recruiters on Yahoo!'s Web Hosting

[13]Dissecting an Ongoing Money Mule Recruitment Campaign

[14]Keeping Money Mule Recruiters on a Short Leash - Part Two

[15]Keeping Reshipping Mule Recruiters on a Short Leash

[16]Keeping Money Mule Recruiters on a Short Leash

[17]Standardizing the Money Mule Recruitment Process

[18]Inside a Money Laundering Group's Spamming Operations

[19]Money Mule Recruiters use ASProx's Fast Fluxing Services

[20]Money Mules Syndicate Actively Recruiting Since 2002

This post has been reproduced from [21]Dancho Danchev's blog.

1. <http://ddanchev.blogspot.com/2011/08/keeping-money-mule-recruiters-on-short.html>

2. <http://ddanchev.blogspot.com/2011/07/keeping-money-mule-recruiters-on-short.html>

3. http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short_30.html

4. http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short_25.html

5. <http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short.html>

6. <http://ddanchev.blogspot.com/2011/03/keeping-money-mule-recruiters-on-short.html>

7. <http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html>

8. <http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html>

9. <http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html>
10. <http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html>
11. <http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html>
12. <http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html>
13. <http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html>
14. <http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html>
15. <http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html>
16. <http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html>

43

17. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>
18. <http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html>
19. <http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asprox-fast.html>
20. <http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html>

21. <http://ddanchev.blogspot.com/>

44



Summarizing Webroot's Threat Blog Posts for December (2013-01-09 19:34)

The following is a brief summary of all of my posts at [1]**Webroot's Threat Blog** for December, 2012. You can

subscribe to [2]**Webroot's Threat Blog RSS Feed**, or follow me on Twitter:

01. [3]DIY malicious domain name registering service spotted in the wild
02. [4]Fake 'FedEx Tracking Number' themed emails lead to malware
03. [5]Bogus 'Facebook Account Cancellation Request' themed emails serve client-side exploits and malware
04. [6]Malicious 'Security Update for Banking Accounts' emails lead to Black Hole Exploit Kit
05. [7]A peek inside a boutique cybercrime-friendly E-shop - part five
06. [8]Fake 'Flight Reservation Confirmations' themed emails lead to Black Hole Exploit Kit
07. [9]Malicious 'Sendspace File Delivery Notifications' lead to Black Hole Exploit Kit

08. [10]Fake Chase 'Merchant Billing Statement' themed emails lead to malware
09. [11]Cybercriminals entice potential cybercriminals into purchasing bogus credit cards data
10. [12]Fake 'Change Facebook Color Theme' events lead to rogue Chrome extensions
11. [13]Fake 'Citi Account Alert' themed emails lead to Black Hole Exploit Kit
12. [14]Spamvertised 'Work at Home' scams impersonating CNBC spotted in the wild
13. [15]Pharmaceutical scammers spamvertise YouTube themed emails, entice users into purchasing counterfeit drugs
14. [16]Cybercriminals resume spamvertising British Airways themed E-ticket receipts, serve malware
15. [17]Fake 'UPS Delivery Confirmation Failed' themed emails lead to Black Hole Exploit Kit

45

16. [18]Webroot's Threat Blog Most Popular Posts for 2012

This post has been reproduced from [19]Dancho Danchev's blog. Follow him [20]on Twitter.

1. <http://blog.webroot.com/>
2. <http://feeds2.feedburner.com/WebrootThreatBlog>

3. <http://blog.webroot.com/2012/12/03/diy-malicious-domain-name-registering-service-spotted-in-the-wild/>
4. <http://blog.webroot.com/2012/12/04/fake-fedex-tracking-number-themed-emails-lead-to-malware/>
5. <http://blog.webroot.com/2012/12/05/bogus-facebook-account-cancellation-request-themed-emails-serve-client-side-exploits-and-malware/>
6. <http://blog.webroot.com/2012/12/07/malicious-security-update-for-banking-accounts-emails-lead-to-black-hole-exploit-kit/>
7. <http://blog.webroot.com/2012/12/10/a-peek-inside-a-boutique-cybercrime-friendly-e-shop-part-five/>
8. <http://blog.webroot.com/2012/12/11/fake-flight-reservation-confirmations-themed-emails-lead-to-black-hole-exploit-kit/>
9. <http://blog.webroot.com/2012/12/12/malicious-sendspace-file-delivery-notifications-lead-to-black-hole-exploit-kit/>
10. <http://blog.webroot.com/2012/12/14/fake-chase-merchant-billing-statement-themed-emails-lead-to-malware/>
11. <http://blog.webroot.com/2012/12/18/cybercriminals-entice-potential-cybercriminals-into-purchasing-bogus-credit-cards-data/>

12. <http://blog.webroot.com/2012/12/19/fake-change-facebook-color-theme-events-lead-to-rogue-chrome-extension>

[s/](#)

13. <http://blog.webroot.com/2012/12/20/fake-citi-account-alert-themed-emails-lead-to-black-hole-exploit-kit/>

14. <http://blog.webroot.com/2012/12/21/spamvertised-work-at-home-scams-impersonating-cnbc-spotted-in-the-wild>

[/](#)

15. <http://blog.webroot.com/2012/12/25/pharmaceutical-scammers-spamvertise-youtube-themed-emails-entice-users-into-purchasing-counterfeit-drugs/>

16. <http://blog.webroot.com/2012/12/26/cybercriminals-resume-spamvertising-british-airways-themed-e-ticket-receipts-serve-malware/>

17. <http://blog.webroot.com/2012/12/27/fake-ups-delivery-confirmation-failed-themed-emails-lead-to-black-hole-exploit-kit/>

18. <http://blog.webroot.com/2012/12/28/webroots-threat-blog-most-popular-posts-for-2012/>

19. <http://ddanchev.blogspot.com/>

20. <http://twitter.com/danchodanchev>

1.2

February

47



Summarizing ZDNet's Zero Day Posts for January (2013-02-04 22:38)

The following is a brief summary of all of my posts at [1]**ZDNet's Zero Day** for January, 2013. You can subscribe to

[2]Zero Day's main feed , or follow me on Twitter:

01. [3]Dutch security researchers dissect the Pobelka botnet

02. [4]ESPN's ScoreCenter for iOS sends passwords in clear-text, susceptible to XSS flaw

03. [5]Report: AutoRun malware infections continue topping the charts

04. [6]Comparative review: Opera leads in browser anti-phishing protection

05. [7]Italian-language page at MSN redirects to Cool Exploit Kit, serves ransomware

06. [8]WordPress releases version 3.5.1, fixes 3 security issues

07. [9]Targeted attack against UAE activist utilizes CVE-2013-0422, drops malware

This post has been reproduced from [10]Dancho Danchev's blog. Follow him [11]on Twitter.

1. <http://zdnet.com/blog/security>

2. <http://feeds.feedburner.com/zdnet/security>

48

3. <http://www.zdnet.com/dutch-security-researchers-dissect-the-pobelka-botnet-7000009971/>

4. <http://www.zdnet.com/espn-scorecenter-for-ios-sends-passwords-in-clear-text-susceptible-to-xss-flaw-7000009976/>

[009976/](http://www.zdnet.com/espn-scorecenter-for-ios-sends-passwords-in-clear-text-susceptible-to-xss-flaw-7000009976/)

5. <http://www.zdnet.com/report-autorun-malware-infections-continue-topping-the-charts-7000010028/>

6. <http://www.zdnet.com/comparative-review-opera-leads-in-browser-anti-phishing-protection-7000010039/>

7. <http://www.zdnet.com/italian-language-page-at-msn-redirects-to-cool-exploit-kit-serves-ransomware-7000010299/>

[299/](http://www.zdnet.com/italian-language-page-at-msn-redirects-to-cool-exploit-kit-serves-ransomware-7000010299/)

8. <http://www.zdnet.com/wordpress-releases-version-3-5-1-fixes-3-security-issues-7000010355/>

9. <http://www.zdnet.com/targeted-attack-against-uae-activist-utilizes-cve-2013-0422-drops-malware-7000010645/>

[/](http://www.zdnet.com/targeted-attack-against-uae-activist-utilizes-cve-2013-0422-drops-malware-7000010645/)

10. <http://ddanchev.blogspot.com/>

11. <http://twitter.com/danchodanchev>

49



Summarizing Webroot's Threat Blog Posts for January (2013-02-04 23:14)

The following is a brief summary of all of my posts at [1]**Webroot's Threat Blog** for January, 2013. You can subscribe to [2]**Webroot's Threat Blog RSS Feed**, or follow me on Twitter:

- 01.** [3]Spamvertised 'Your Recent eBill from Verizon Wireless' themed emails serve client-side exploits and malware
- 02.** [4]Fake BBB (Better Business Bureau) Notifications lead to Black Hole Exploit Kit
- 03.** [5]'Attention! Changes in the bank reports!' themed emails lead to Black Hole Exploit Kit
- 04.** [6]Fake 'You have made an Ebay purchase' themed emails lead to client-side exploits and malware
- 05.** [7]A peek inside a boutique cybercrime-friendly E-shop – part six
- 06.** [8]Black Hole Exploit Kit author's 'vertical market integration' fuels growth in malicious Web activity
- 07.** [9]Spamvertised AICPA themed emails serve client-side exploits and malware

08. [10]'Please confirm your U.S Airways online registration' themed emails lead to Black Hole Exploit Kit

09. [11]Malicious DIY Java applet distribution platforms going mainstream

10. [12]Fake 'ADP Speedy Notifications' lead to client-side exploits and malware

11. [13]Cybercriminals release automatic CAPTCHA-solving bogus Youtube account generating tool

12. [14]'Batch Payment File Declined' EFTPS themed emails lead to Black Hole Exploit Kit

50

13. [15]Cybercriminals resume spamvertising fake Vodafone 'A new picture or video message' themed emails, serve malware

14. [16]Leaked DIY malware generating tool spotted in the wild

15. [17]Email hacking for hire going mainstream – part three

16. [18]Android malware spreads through compromised legitimate Web sites

17. [19]Fake Intuit 'Direct Deposit Service Informer' themed emails lead to Black Hole Exploit Kit

18. [20]Fake LinkedIn 'Invitation Notifications' themed emails lead to client-side exploits and malware

19. [21]Novice cybercriminals experiment with DIY ransomware tools

20. [22]Bogus 'Your Paypal Transaction Confirmation' themed emails lead to Black Hole Exploit Kit

21. [23]Fake 'FedEx Online Billing – Invoice Prepared to be Paid' themed emails lead to Black Hole Exploit Kit

22. [24]A peek inside a DIY password stealing malware

23. [25]Malicious 'Facebook Account Cancellation Request' themed emails serve client-side exploits and malware

This post has been reproduced from [26]Dancho Danchev's blog. Follow him [27]on Twitter.

1. <http://blog.webroot.com/>

2. <http://feeds2.feedburner.com/WebrootThreatBlog>

3. <http://blog.webroot.com/2013/01/01/spamvertised-your-recent-ebill-from-verizon-wireless-themed-emails-serve-client-side-exploits-and-malware/>

4. <http://blog.webroot.com/2013/01/02/fake-bbb-better-business-bureau-notifications-lead-to-black-hole-exploit-kit/>

5. <http://blog.webroot.com/2013/01/03/attention-changes-in-the-bank-reports-themed-emails-lead-to-black-hole-exploit-kit/>

6. <http://blog.webroot.com/2013/01/04/fake-you-have-made-an-ebay-purchase-themed-emails-lead-to-client-side-exploits-and-malware/>

7. <http://blog.webroot.com/2013/01/07/a-peek-inside-a-boutique-cybercrime-friendly-e-shop-part-six/>

8. <http://blog.webroot.com/2013/01/08/black-hole-exploit-kit-authors-vertical-market-integration-fuels-growth-in-malicious-web-activity/>

9. <http://blog.webroot.com/2013/01/09/spamvertised-aicpa-themed-emails-serve-client-side-exploits-and-malware/>

10. <http://blog.webroot.com/2013/01/10/please-confirm-your-u-s-airways-online-registration-themed-emails-lead-to-black-hole-exploit-kit/>

11. <http://blog.webroot.com/2013/01/11/malicious-diy-java-applet-distribution-platforms-going-mainstream/>

12. <http://blog.webroot.com/2013/01/14/fake-adp-speedy-notifications-lead-to-client-side-exploits-and-malware/>

13. <http://blog.webroot.com/2013/01/15/cybercriminals-release-automatic-captcha-solving-bogus-youtube-account-generating-tool/>

14. <http://blog.webroot.com/2013/01/16/batch-payment-file-declined-eftps-themed-emails-lead-to-black-hole-exploit-kit/>

15. <http://blog.webroot.com/2013/01/17/cybercriminals-resume-spamvertising-fake-vodafone-a-new-picture-or-video-message-themed-emails-serve-malware/>
16. <http://blog.webroot.com/2013/01/18/leaked-diy-malware-generating-tool-spotted-in-the-wild/>
17. <http://blog.webroot.com/2013/01/21/email-hacking-for-hire-going-mainstream-part-three/>
18. <http://blog.webroot.com/2013/01/22/android-malware-spreads-through-compromised-legitimate-web-sites/>
19. <http://blog.webroot.com/2013/01/23/fake-intuit-direct-deposit-service-informer-themed-emails-lead-to-black-hole-exploit-kit/>
20. <http://blog.webroot.com/2013/01/24/fake-linkedin-invitation-notifications-themed-emails-lead-to-client-side-exploits-and-malware/>
21. <http://blog.webroot.com/2013/01/25/novice-cybercriminals-experiment-with-diy-ransomware-tools/>

51

22. <http://blog.webroot.com/2013/01/28/bogus-your-paypal-transaction-confirmation-themed-emails-lead-to-black-hole-exploit-kit/>

23.

<http://blog.webroot.com/2013/01/29/fake-fedex-online-billing-invoice-prepared-to-be-paid-themed-emails->

[lead-to-black-hole-exploit-kit/](#)

24. <http://blog.webroot.com/2013/01/30/a-peek-inside-a-diy-password-stealing-malware/>

25. <http://blog.webroot.com/2013/01/31/malicious-facebook-account-cancellation-request-themed-emails-serve-cl>

[ient-side-exploits-and-malware/](#)

26. <http://ddanchev.blogspot.com/>

27. <http://twitter.com/danchodanchev>

52



Historical OSINT - Hacked Databases Offered for Sale (2013-02-06 02:03)

In the wake of the recently announced security breaches at the [1]**NYTimes**, [2]**WSJ**, and the [3]**Washington Post**, I decided to shed more light on what happens once a database gets compromised by Russian cybercriminals,

compared to (supposedly) Chinese spies, with the idea to provide factual evidence that these breaches are just the

tip of the iceberg.

In this intelligence brief, I'll profile a service that was originally operating throughout the entire 2009, selling

access to compromised databases of multiple high-trafficked Web sites, through the direct compromise of their

databases, hence, the name of the service - GiveMeDB.

Primary URL: *hxxp://givemedb.com* - Email: *giverems@mail.ru*

Secondary URL: *hxxp://shopdb.blogspot.com*

53

ICQ: *9348793; 5190451*

During 2009, the domain used to respond to **83.133.123.228** (LAMBDANET-AS European Backbone of LambdaNet),

it then changed IPs to **74.54.82.209** (THEPLANET-AS - ThePlanet.com Internet Services, Inc.). The following domains

used to respond to the same IP (**83.133.123.228**), **pornofotki.com.ua**, **mail.vipnkvd.ru**. What are the chances that these IPs are known to have been involved in related malicious/cybercrime-friendly activities? Appreciate my rhetoric.

We've got the following [4]**MD5:**

6a9b128545bd095dbbb697756f5586a9 spamming links to the same

(**hxxp://83.133.123.228/uksus/?t=3**) in particular.

Cross-checking the second IP (**74.54.82.209**) across multiple proprietary and public databases, reveals a diversified criminal enterprise that's been using it for years.

The following MD5s are known to have phoned back to the same IP (**74.54.82.209**):

[5]**MD5: d48a7ae9934745964951a704bcc70fe9**

[6]**MD5: 4626de911152ae7618c9936d8d258577**

[7]**MD5: ca4b79a33ea6e311eafa59a6c3fffee2**

[8]**MD5: eb3b44cee34ec09ec6c5917c5bd7cfb4**

As well as a recent (2011) [9]**Palevo C &C activity**. Clearly, they've been multi-tasking on multiple fronts.

The structure of propositions is the following: partial URL of the hacked Web site, country of the Web site,

Quantity of records per database, First-time price, Exclusive price. The list of affected Web sites is as follows:

54



Job/CV Databases:

*jobsbazaar.**

*availablejobs.**

*ecarers.**

*fecareers.**

*healthmeet.**

*youths.**

*jobpilot.**

*thecareerengineer.**

*iauk.**

*jobboerse.**

*creativepool.**

*jobsinkent.**

*jobsinthemoney.**

*jobup.**

*rxcareercenter.**

55



Dating Databases:

*freedating.**

*singles-bar.**

*muenchner-singles.**

*dateclub.**

*websingles.**

*find-you.**

*fitness-singles.**

*houstonconnect.**

*datingz.**

*loveandfriends.**

*lovebyrd.**

56



*mydatingplacephx.**

*cozydating.**

*singletreffen.**

*datearea.**

*endless-fantasy.**

Financial Databases:

*importers.**

*money.**

*pcquote.**

*investorvillage.**

*gurufocus.**

*individual.**

57



*arabianbusiness.**

*ecademy.**

Other Databases:

*pokersourceonline.**

*wickedcolors.**

*salespider.**

*busytrade.**

*funky.**

Purchasing these hacked databases, immediately improves the competitiveness of a potential cybercriminal,

who now has everything he/she needs to launch spam, spear phishing, and [10]**money mule recruitment campaigns**,

at their disposal.

For years, novice cybercriminals or unethical competitors have been on purposely joining closed cybercrime-

friendly communities, seeking help in exchange for a financial incentive, in obtaining access to a particular database,

or for the "[11]**defacement**" of a specific Web site. What this service proves is that, the model can actually scale to 58

disturbing proportions, offering access to millions of compromised database records to virtually anyone who pays for them.

This post has been reproduced from [12]Dancho Danchev's blog. Follow him [13]on Twitter.

1.

http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?pagewanted=all&_r=0

2.

<http://professional.wsj.com/article/SB10001424127887323926104578276202952260718.html>

3.

http://www.washingtonpost.com/business/technology/chinese-hackers-suspected-in-attack-on-the-posts-computers/2013/02/01/d5a44fde-6cb1-11e2-bd36-c0fe61a205f6_story.html

4.

<https://www.virustotal.com/file/131f2f8870071f490baf268fd3becc02b8a4dc755b23c3853e04d413a4987f6a/analysis/>

5.

<https://www.virustotal.com/file/30a5441a26461e9ffc86187a0c2f6574d51d27a52a6188ecbba50cc2345586c9/analysis/>

6.

<https://www.virustotal.com/file/f06867926bcff4641d1308acdb7fddf1b99f9babaca83bb72e811f1345f8904b/analysis/>

7.

<https://www.virustotal.com/file/62e36c696c8bff15ba6a1b58774485ca4f18c704af9410495b4b7d24fe437901/analysis/>

8.

<https://www.virustotal.com/file/99d2cbdee78f7d66d73e7545e6e03d0f20f2d731f9911fdd84c4c95f6ddea9b7/analysis/>

9. <https://palevotracker.abuse.ch/?ipaddress=74.54.82.209>
10. <https://www.google.com/webhp?hl=en&tab=ww&authuser=0#hl=en&tbo=d&authuser=0&sclient=psy-ab&q=site:ddanchev.blogspot.com+%22money+mule%22&oq=site:ddanchev.blogspot>
11. <http://ddanchev.blogspot.com/2008/04/commercial-web-site-defacement-tool.html>
12. <http://ddanchev.blogspot.com/>
13. <http://twitter.com/danchodanchev>

59



Historical OSINT - Hacked Databases Offered for Sale (2013-02-06 02:03)

In the wake of the recently announced security breaches at the [1]**NYTimes**, [2]**WSJ**, and the [3]**Washington Post**, I decided to shed more light on what happens once a database gets compromised by Russian cybercriminals,

compared to (supposedly) Chinese spies, with the idea to provide factual evidence that these breaches are just the tip of the iceberg.

In this intelligence brief, I'll profile a service that was originally operating throughout the entire 2009, selling

access to compromised databases of multiple high-trafficked Web sites, through the direct compromise of their

databases, hence, the name of the service - GiveMeDB.

Primary URL: *hxxp://givemedb.com* - Email: *giverems@mail.ru*

60

Secondary URL: *hxxp://shopdb.blogspot.com*

ICQ: *9348793; 5190451*

During 2009, the domain used to respond to **83.133.123.228** (LAMBDANET-AS European Backbone of LambdaNet),

it then changed IPs to **74.54.82.209** (THEPLANET-AS - ThePlanet.com Internet Services, Inc.). The following domains

used to respond to the same IP (**83.133.123.228**), **pornofotki.com.ua**, **mail.vipnkvd.ru**. What are the chances that these IPs are known to have been involved in related malicious/cybercrime-friendly activities? Appreciate my rhetoric.

We've got the following [4]**MD5:**

6a9b128545bd095dbbb697756f5586a9 spamming links to the same

(**hxxp://83.133.123.228/uksus/?t=3**) in particular.

Cross-checking the second IP (**74.54.82.209**) across multiple proprietary and public databases, reveals a diversified criminal enterprise that's been using it for years.

The following MD5s are known to have phoned back to the same IP (**74.54.82.209**):

[5]**MD5: d48a7ae9934745964951a704bcc70fe9**

[6]**MD5: 4626de911152ae7618c9936d8d258577**

[7]**MD5: ca4b79a33ea6e311eafa59a6c3fffee2**

[8]**MD5: eb3b44cee34ec09ec6c5917c5bd7cfb4**

As well as a recent (2011) [9]**Palevo C &C activity**. Clearly, they've been multi-tasking on multiple fronts.

The structure of propositions is the following: partial URL of the hacked Web site, country of the Web site,

Quantity of records per database, First-time price, Exclusive price. The list of affected Web sites is as follows:

61



Job/CV Databases:

*jobsbazaar.**

*availablejobs.**

*ecarers.**

*fecareers.**

*healthmeet.**

*youths.**

*jobpilot.**

*thecareerengineer.**

*iauk.**

*jobboerse.**

*creativepool.**

*jobsinkent.**

*jobsinthemoney.**

*jobup.**

*rxcareercenter.**

62



Dating Databases:

*freedating.**

*singles-bar.**

*muenchner-singles.**

*dateclub.**

*websingles.**

*find-you.**

*fitness-singles.**

*houstonconnect.**

*datingz.**

*loveandfriends.**

*lovebyrd.**

*mydatingplacephx.**

63



*cozydating.**

*singletreffen.**

*datearea.**

*endless-fantasy.**

Financial Databases:

*importers.**

*money.**

*pcquote.**

*investorvillage.**

*gurufocus.**

*individual.**

*arabianbusiness.**

*ecademy.**

64



Other Databases:

*pokersourceonline.**

*wickedcolors.**

*salespider.**

*busytrade.**

*funky.**

Purchasing these hacked databases, immediately improves the competitiveness of a potential cybercriminal,

who now has everything he/she needs to launch spam, spear phishing, and [10]**money mule recruitment campaigns**,

at their disposal.

For years, novice cybercriminals or unethical competitors have been on purposely joining closed cybercrime-

friendly communities, seeking help in exchange for a financial incentive, in obtaining access to a particular database,

or for the "[11]**defacement**" of a specific Web site. What this service proves is that, the model can actually scale to disturbing proportions, offering access to millions of compromised database records to virtually anyone who pays for them.

Updates will be posted as soon as new developments take place.

1.

http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?pagewanted=all&_r=0

2.

<http://professional.wsj.com/article/SB10001424127887323926104578276202952260718.html>

3.

http://www.washingtonpost.com/business/technology/chinese-hackers-suspected-in-attack-on-the-posts-computers/2013/02/01/d5a44fde-6cb1-11e2-bd36-c0fe61a205f6_story.html

4.

<https://www.virustotal.com/file/131f2f8870071f490baf268fd3becc02b8a4dc755b23c3853e04d413a4987f6a/analysis/>

5.

<https://www.virustotal.com/file/30a5441a26461e9ffc86187a0c2f6574d51d27a52a6188ecbba50cc2345586c9/analysis/>

6.

<https://www.virustotal.com/file/f06867926bcff4641d1308acdb7fddf1b99f9babaca83bb72e811f1345f8904b/analysis/>

7.

<https://www.virustotal.com/file/62e36c696c8bff15ba6a1b58774485ca4f18c704af9410495b4b7d24fe437901/analysis/>

8.

<https://www.virustotal.com/file/99d2cbdee78f7d66d73e7545e6e03d0f20f2d731f9911fdd84c4c95f6ddea9b7/analysis/>

9. <https://palevotracker.abuse.ch/?ipaddress=74.54.82.209>

10. <https://www.google.com/webhp?hl=en&tab=ww&authuser=0#hl=en&tbo=d&authuser=0&sclient=psy-ab&q=site:ddanchev>

[.blogspot.com+%22money+mule%22&oq=site:ddanchev.blogspot.com](https://www.google.com/search?q=site:ddanchev.blogspot.com+%22money+mule%22&oq=site:ddanchev.blogspot.com)

11. <http://ddanchev.blogspot.com/2008/04/commercial-web-site-defacement-tool.html>

66



Dissecting NBC's Exploits and Malware Serving Web Site Compromise (2013-02-21 22:03)

The web site of the [1]**National Broadcasting Company (NBC)**, NBC.com, is currently compromised, and is redi-

recting tens of thousands of legitimate users to multiple exploits serving and malware dropping malicious URLs.

The campaign appears to have been launched by the same gang of cybercriminals that's also been recently in-

involved in impersonating [2]**Facebook Inc.** and [3]**Verizon Wireless**, in an attempt to trick their users/customers into clicking on links found in hundreds of thousands of spamvertised emails pretending to come from the companies.

Let's dissect the campaign, expose its structure, the dropped malware, and connect the dots on who's behind it.

Observed iFrames in rotation:

hxxp://umaiskhan.com/znzd.html

hxxp://umaiskhan.com/ztuj.html

hxxp://priceworldpublishing.com/aynk.html

hxxp://toplineops.com/mtnk.html

hxxp://moi-npovye-sploett.com/qqqq/1.php

hxxp://www.jaylenosgarage.com/trucks/PHP/google.php

hxxp://nikweinstein.com/cl/google.php

Observed redirections leading to:

hxxp://gonullersultani.net/znzd.htm

hxxp://erabisnis.net/znzd.htm

hxxp://electricianfortwayne.info/62.html

hxxp://moi-npovye-sploett.com/cGeQc0wz1KPI/larktion.php

67



Sample client-side exploitation chain for the first campaign:

hxxp://toplineops.com/mtnk.html ->

hxxp://electricianfortwayne.info/62.html ->

hxxp://electricianfortwayne.info/987.pdf

Upon successful client-side exploitation, the campaign drops [4]**MD5: 4e48ddc2a2481f9ff27113e6395160e1** -

detected by 7 out of 46 antivirus scanners as Trojan-Spy.Win32.Zbot.jfgj.

Once executed the sample creates the "Xi3FVnelx" Mutex and phones back to:

hxxp://eastsidetennisassociation.com/i.htm?

jzd63F1JyFUfMyyf1Q8U9 - 74.220.215.229

hxxp://envirsoft.com/n.htm?

xWasESNrgozQ13QNR1PNCGTGhPAW16QJ67Bnj

-

174.120.29.2

-

Email:

louis.bouchard@envirsoft.com

hxxp://beautiesofcanada.com/s.htm?

2dIYtfCwTLfFBzTL8TrY7btwJDVszOI

-

66.96.145.104

-

Email:

ed-

dom@yahoo.com

68



hxxp://magasin-shop.com/v.htm?

ZPlkcqLyyHFRxHmhVxQN8HdfszymBrXxuy - 66.96.160.143

hxxp://couche-transport.comlu.com/r.htm?

Mb6kKF3mq5H8YxeVXYM9yOwK - 31.170.161.96

Second

redirection

redirection

chain

for

a

sampled

iFrame:

hxxp://moi-npovye-

sploett.com/qqqq/1.php -> hxxp://moi-npovye-

sploett.com/cGeQc0wz1KPl/larktion.php -> hxxp://moi-

npovye-sploett.com/cGeQc0wz1KPl/aflybing.php?

esusvity=78528 0 where it attempts to exploit [5]**CVE-**

2010-0188.

Malicious domains reconnaissance:

umaiskhan.com - 173.254.28.49 - Email:
chfaisal009@gmail.com - appears to be a compromised site
belonging to

someone named "Azhar Mahmood", unless of course you
want to believe that Pakistan's cyber warfare unit is behind
the campaign, since this is the second time that I come
across to this IP. Keep reading!

priceworldpublishing.com - 174.122.45.74 - Email:
info@sportsworkout.com

electricianfortwayne.info - 173.201.92.1 - Email:
mdkline65@yahoo.com

gonullersultani.net - 72.167.2.128 - Email:
gonullersultani@gmail.com

erabisnis.net - 74.220.207.161

moi-npovye-sploett.com - 130.185.157.102 - Email:
josephhaddad829@yahoo.com

jaylenosgarage.com - 80.239.148.217

nikweinstein.com - 205.178.145.95 - Email:
nikweinstein@hotmail.com

**mdkline65@yahoo.com is also known to have
registered the following domains:**

dedirt.com

dogsrit.com

spiritualspice.us

madamerufus.com

herbalstatelegal.com

myauditionsite.com

injurylawyercleveland.info

injurylawyerspringfieldmo.info

injurylawyercolumbus.info

injurylawyerindianapolis.info

69

Who's behind this campaign and can we connect this malicious activities to previously analyzed malicious campaigns?

But, of course.

umaiskhan.com responds to 173.254.28.49, and on 2013-01-28 18:56:19 we know that another domain used

in a Facebook Inc. themed campaign was also responding to the same IP, namely **hxxp://shutterstars.com/wp-**

content/plugins/akismet/resume_facebook.html. The compromised legitimate host back then used to serve

client-side exploits through

hxxp://gotina.net/detects/sign_on_to_resume.php - 222.238.109.66 - Email:

lockwr@rocketmail.com.

Deja vu! We've already seen and profiled this malicious domain in the following assessment "[6]**Fake 'You've**

blocked/disabled your Facebook account' themed emails serve client-side exploits and malware", indicating that both of these campaigns have been launched by the same cybercriminal/gang of cybercriminals. What's also worth

emphasizing on is that the same email (*lockwr@rocketmail.com*) used to register gonita.net was also profiled in the following assessment "[7]**Fake 'Verizon Wireless Statement' themed emails lead to Black Hole Exploit Kit"**, where it was used to register the Name Servers used in the campaign.

Someone's multi-tasking. That's for sure.

This post has been reproduced from [8]Dancho Danchev's blog. Follow him [9]on Twitter.

1. <http://en.wikipedia.org/wiki/NBC>
2. <http://blog.webroot.com/tag/facebook/>
3. <http://blog.webroot.com/tag/verizon/>
4. <https://www.virustotal.com/en/file/6b276bee21bf5946461e3c62f447b3be7179e9cce4742a61b26417609ed001ee/analysis/>
5. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0188>

6. <http://blog.webroot.com/2013/02/14/fake-youve-blockeddisabled-your-facebook-account-themed-emails-serve-c>

[lient-side-exploits-and-malware/](#)

7. <http://blog.webroot.com/2013/02/21/fake-verizon-wireless-statement-themed-emails-lead-to-black-hole-exploit-kit/>

8. <http://ddanchev.blogspot.com/>

9. <http://twitter.com/danchodanchev>

70



Dissecting NBC's Exploits and Malware Serving Web Site Compromise (2013-02-21 22:03)

The web site of the [1]**National Broadcasting Company (NBC)**, NBC.com, is currently compromised, and is redi-

recting tens of thousands of legitimate users to multiple exploits serving and malware dropping malicious URLs.

The campaign appears to have been launched by the same gang of cybercriminals that's also been recently in-

involved in impersonating [2]**Facebook Inc.** and [3]**Verizon Wireless**, in an attempt to trick their users/customers into clicking on links found in hundreds of thousands of spamvertised emails pretending to come from the companies.

Let's dissect the campaign, expose its structure, the dropped malware, and connect the dots on who's behind it.

Observed iFrames in rotation:

hxxp://umaiskhan.com/znzd.html

hxxp://umaiskhan.com/ztuj.html

hxxp://priceworldpublishing.com/aynk.html

hxxp://toplineops.com/mtnk.html

hxxp://moi-npovye-sploett.com/qqqq/1.php

hxxp://www.jaylenosgarage.com/trucks/PHP/google.php

hxxp://nikweinstein.com/cl/google.php

Observed redirections leading to:

hxxp://gonullersultani.net/znzd.htm

hxxp://erabisnis.net/znzd.htm

hxxp://electricianfortwayne.info/62.html

hxxp://moi-npovye-sploett.com/cGeQc0wz1KPI/larktion.php

71



Sample client-side exploitation chain for the first campaign:

hxxp://toplineops.com/mtnk.html ->

hxxp://electricianfortwayne.info/62.html ->

hxxp://electricianfortwayne.info/987.pdf

Upon successful client-side exploitation, the campaign drops [4]**MD5: 4e48ddc2a2481f9ff27113e6395160e1** -

detected by 7 out of 46 antivirus scanners as Trojan-Spy.Win32.Zbot.jfgj.

Once executed the sample creates the "Xi3FVnelx" Mutex and phones back to:

hxxp://eastsidetennisassociation.com/i.htm?

jzd63F1JyFUfMyyf1Q8U9 - 74.220.215.229

hxxp://envirsoft.com/n.htm?

xWasESNrgozQ13QNR1PNCGTGhPAW16QJ67Bnj

-

174.120.29.2

-

Email:

louis.bouchard@envirsoft.com

hxxp://beautiesofcanada.com/s.htm?

2dIYtfCwTLfFBzTL8TrY7btwJDVszOI

-

66.96.145.104

-

Email:

ed-

dom@yahoo.com

72



hxxp://magasin-shop.com/v.htm?

ZPlkcqLyyHFRxHmhVxQN8HdfszymBrXxuy - 66.96.160.143

hxxp://couche-transport.comlu.com/r.htm?

Mb6kKF3mq5H8YxeVXYM9yOwK - 31.170.161.96

Second

redirection

redirection

chain

for

a

sampled

iFrame:

hxxp://moi-npovye-

sploett.com/qqqq/1.php -> hxxp://moi-npovye-

sploett.com/cGeQc0wz1KPl/larktion.php -> hxxp://moi-

npovye-sploett.com/cGeQc0wz1KPl/aflybing.php?

esusvity=78528 0 where it attempts to exploit [5]**CVE-**

2010-0188.

Malicious domains reconnaissance:

umaiskhan.com - 173.254.28.49 - Email:
chfaisal009@gmail.com - appears to be a compromised site
belonging to

someone named "Azhar Mahmood", unless of course you
want to believe that Pakistan's cyber warfare unit is behind
the campaign, since this is the second time that I come
across to this IP. Keep reading!

priceworldpublishing.com - 174.122.45.74 - Email:
info@sportsworkout.com

electricianfortwayne.info - 173.201.92.1 - Email:
mdkline65@yahoo.com

gonullersultani.net - 72.167.2.128 - Email:
gonullersultani@gmail.com

erabisnis.net - 74.220.207.161

moi-npovye-sploett.com - 130.185.157.102 - Email:
josephhaddad829@yahoo.com

jaylenosgarage.com - 80.239.148.217

nikweinstein.com - 205.178.145.95 - Email:
nikweinstein@hotmail.com

**mdkline65@yahoo.com is also known to have
registered the following domains:**

dedirt.com

dogsrit.com

spiritualspice.us

madamerufus.com

herbalstatelegal.com

myauditionsite.com

injurylawyercleveland.info

injurylawyerspringfieldmo.info

injurylawyercolumbus.info

injurylawyerindianapolis.info

73

Who's behind this campaign and can we connect this malicious activities to previously analyzed malicious campaigns?

But, of course.

umaiskhan.com responds to 173.254.28.49, and on 2013-01-28 18:56:19 we know that another domain used

in a Facebook Inc. themed campaign was also responding to the same IP, namely **hxxp://shutterstars.com/wp-**

content/plugins/akismet/resume_facebook.html. The compromised legitimate host back then used to serve

client-side exploits through

hxxp://gotina.net/detects/sign_on_to_resume.php - 222.238.109.66 - Email:

lockwr@rocketmail.com.

Deja vu! We've already seen and profiled this malicious domain in the following assessment "[6]**Fake 'You've**

blocked/disabled your Facebook account' themed emails serve client-side exploits and malware", indicating that both of these campaigns have been launched by the same cybercriminal/gang of cybercriminals. What's also worth

emphasizing on is that the same email (*lockwr@rocketmail.com*) used to register gonita.net was also profiled in the following assessment "[7]**Fake 'Verizon Wireless Statement' themed emails lead to Black Hole Exploit Kit"**, where it was used to register the Name Servers used in the campaign.

Someone's multi-tasking. That's for sure.

Updates will be posted as soon as new developments take place.

1. <http://en.wikipedia.org/wiki/NBC>
2. <http://blog.webroot.com/tag/facebook/>
3. <http://blog.webroot.com/tag/verizon/>
4. <https://www.virustotal.com/en/file/6b276bee21bf5946461e3c62f447b3be7179e9cce4742a61b26417609ed001ee/analysis/>
5. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0188>

6. <http://blog.webroot.com/2013/02/14/fake-youve-blockeddisabled-your-facebook-account-themed-emails-serve-c>

[lient-side-exploits-and-malware/](#)

7. <http://blog.webroot.com/2013/02/21/fake-verizon-wireless-statement-themed-emails-lead-to-black-hole-explo>

[it-kit/](#)

74

1.3

March

75



Summarizing Webroot's Threat Blog Posts for February (2013-03-04 15:31)

The following is a brief summary of all of my posts at [1]**Webroot's Threat Blog** for February, 2013. You can subscribe to [2]**Webroot's Threat Blog RSS Feed**, or follow me on Twitter:

01. [3]Fake Booking.com 'Credit Card was not Accepted' themed emails lead to malware

02. [4]Fake FedEx 'Tracking ID/Tracking Number/Tracking Detail' themed emails lead to malware

03. [5]'Your Kindle e-book Amazon receipt' themed emails lead to Black Hole Exploit Kit

- 04.** [6]New DIY HTTP-based botnet tool spotted in the wild
- 05.** [7]Mobile spammers release DIY phone number harvesting tool
- 06.** [8]New underground service offers access to thousands of malware-infected hosts
- 07.** [9]Targeted 'phone ring flooding' attacks as a service going mainstream
- 08.** [10]Fake 'You've blocked/disabled your Facebook account' themed emails serve client-side exploits and malware
- 09.** [11]Spamvertised IRS 'Income Tax Refund Turned Down' themed emails lead to Black Hole Exploit Kit
- 10.** [12]Malware propagates through localized Facebook Wall posts
- 11.** [13]Malicious 'RE: Your Wire Transfer' themed emails serve client-side exploits and malware

76

- 12.** [14]New underground E-shop offers access to hundreds of hacked PayPal accounts
- 13.** [15]Fake 'Verizon Wireless Statement' themed emails lead to Black Hole Exploit Kit
- 14.** [16]DIY malware cryptor as a Web service spotted in the wild
- 15.** [17]Malicious 'Data Processing Service' ACH File ID themed emails serve client-side exploits and malware

16. [18]How mobile spammers verify the validity of harvested phone numbers

17. [19]How much does it cost to buy 10,000 U.S.-based malware-infected hosts?

This post has been reproduced from [20]Dancho Danchev's blog. Follow him [21]on Twitter.

1. <http://blog.webroot.com/>
2. <http://feeds2.feedburner.com/WebrootThreatBlog>
3. <http://blog.webroot.com/2013/02/01/fake-booking-com-credit-card-was-not-accepted-themed-emails-lead-to-malware/>
4. <http://blog.webroot.com/2013/02/04/fake-fedex-tracking-idtracking-numbertracking-detail-themed-emails-lead-to-malware/>
5. <http://blog.webroot.com/2013/02/05/your-kindle-e-book-amazon-receipt-themed-emails-lead-to-black-hole-exploit-kit/>
6. <http://blog.webroot.com/2013/02/06/new-diy-http-based-botnet-tool-spotted-in-the-wild/>
7. <http://blog.webroot.com/2013/02/07/mobile-spammers-release-diy-phone-number-harvesting-tool/>
8. <http://blog.webroot.com/2013/02/12/new-underground-service-offers-access-to-thousands-of-malware-infected-hosts/>

9. <http://blog.webroot.com/2013/02/13/targeted-phone-ring-flooding-attacks-as-a-service-going-mainstream/>

10. <http://blog.webroot.com/2013/02/14/fake-youve-blockeddisabled-your-facebook-account-themed-emails-serve-c>

[lient-side-exploits-and-malware/](http://blog.webroot.com/2013/02/14/fake-youve-blockeddisabled-your-facebook-account-themed-emails-serve-client-side-exploits-and-malware/)

11.

<http://blog.webroot.com/2013/02/15/spamvertised-irs-income-tax-refund-turned-down-themed-emails-lead-to>

[-black-hole-exploit-kit/](http://blog.webroot.com/2013/02/15/spamvertised-irs-income-tax-refund-turned-down-themed-emails-lead-to-black-hole-exploit-kit/)

12. <http://blog.webroot.com/2013/02/18/malware-propagates-through-localized-facebook-wall-posts/>

13. <http://blog.webroot.com/2013/02/19/malicious-re-your-wire-transfer-themed-emails-serve-client-side-exploi>

[ts-and-malware/](http://blog.webroot.com/2013/02/19/malicious-re-your-wire-transfer-themed-emails-serve-client-side-exploits-and-malware/)

14.

<http://blog.webroot.com/2013/02/20/new-underground-e-shop-offers-access-to-hundreds-of-hacked-paypal-accounts/>

15. <http://blog.webroot.com/2013/02/21/fake-verizon-wireless-statement-themed-emails-lead-to-black-hole-exploit-kit/>

16. <http://blog.webroot.com/2013/02/22/diy-malware-cryptor-as-a-web-service-spotted-in-the-wild/>

17. <http://blog.webroot.com/2013/02/25/malicious-data-processing-service-ach-file-id-themed-emails-serve-client-side-exploits-and-malware/>

18. <http://blog.webroot.com/2013/02/27/how-mobile-spammers-verify-the-validity-of-harvested-phone-numbers/>

19. <http://blog.webroot.com/2013/02/28/how-much-does-it-cost-to-buy-10000-u-s-based-malware-infected-hosts/>

20. <http://ddanchev.blogspot.com/>

21. <http://twitter.com/danchodanchev>

77



Dissecting NBC's Late Night with Jimmy Fallon Web Site Compromise (2013-03-07 00:52)

[1]Oops, they did it again!

The official Web site (***hxxp://www.latenightwithjimmyfallon.com***) of [2]**NBC's Late Night With Jimmy Fallon** is currently [3]**compromised/hacked** and is automatically serving multiple Java exploits to its visitors through a tiny iFrame element embedded on the front page. According to [4]**Google's Safe Browsing Diagnostic page**, the same malicious iFrame domain that affected the Web site, is also known to have affected 15 more domains.

Let's dissect the campaign, expose the complete domains domains portfolio used in the campaign, reproduce the malicious payload, and establish a direct connection between this campaign, and a series of phishing campaigns that appear to have been launched by the same cybercriminal/gang of cybercriminals.

Sample

client-side

exploitation

chain:

hxxp://20-monkeys-b.com/exp/agencept.php?vialjack=339214

-

144.135.8.182; 192.154.103.66 -> hxxp://20-monkeys-b.com/exp/tionjett.php

Although the currently embedded iFrame domain is offline, we know that on 2013-03-06 17:02:35 it used to

respond to 192.154.103.66. We've got several malicious domains currently parked at the same IP and respon-

ing, allowing us to obtain the malicious payload used in the campaign affecting NBC's Web site. Upon further

examination, the obtained malicious PDF used in the campaign, also attempts to connect to the initial iFrame do-

main (**20-monkeys-b.com**), proving that the domains are operated by the same cybercriminal/gang of cybercriminals.

Sample exploitation chain for a currently active malicious domain responding to 192.154.103.66:

hxxp://poople-

78

*huelytics.com/exp/agencept.php?vialjack=694842 ->
hxxp://poople-huelytics.com/exp/addajapa/jurylamp.jar ->
hxxp://poople-huelytics.com/exp/addajapa/ptlyable.jar ->
hxxp://poople-huelytics.com/exp/jectrger.php*

Sample client-side exploits served: [5] *CVE-2013-0431*;
[6] *CVE-2012-1723*; [7] *CVE-2010-0188*

Sample detection rates for the reproduced malicious payload:

test.pdf - [8]**MD5:**

013ed8ef6d92cfe337d9d82767f778da - detected by 10 out of 46 antivirus scanners as

PDF:Exploit.PDF-JS.VU

jurylamp.jar - [9]**MD5:**

dcba86395938737b058299b8e22b6d65 - detected by 7

out of 46 antivirus scanners as

Exploit:Java/CVE-2013-0431

ptlyable.jar - [10]**MD5:**

2446aa6594fc7935ca13b130d4f67442 - detected by 6
out of 46 antivirus scanners as

HEUR:Exploit.Java.CVE-2012-1723.gen

test.pdf drops **MD5:**

51311FDECCD8B6BC5059BE33E0046A27 and **MD5:**
72B670F4582BC73C0D05FF506B51B8EB it

then attempts to obtain the malicious payload from **20-monkeys-b.com/exp/senccute.php?** (144.135.8.182)

Responding to 192.154.103.66 are also the following malicious domains:

snova-vdel-e.com

mimemimikat.info

Malicious domain names reconnaissance:

20-monkeys-b.com - Email: haneslyndsey@yahoo.com

poople-huelytics.com - Email: brianmyhalyk@yahoo.com

snova-vdel-e.com - Email: guerin_k@yahoo.com

mimemimikat.info - Email: xbroshost@live.com

More domains share the same exploitation directory structure (agencept.php?vialjack=) such as for instance:

*hxxp://upd.pes2020.com.ar/up/agencept.php?vialjack
%3D219215*

*hxxp://upd.typescript.com.ar/up/agencept.php?
vialjack=219215*

*hxxp://4ad32203.dyndns.info/agencept.php?
vialjack=428181*

*hxxp://4ad34364.dyndns.info/agencept.php?
vialjack=428181*

*hxxp://4ad28306.dyndns.info/agencept.php?
vialjack=428181*

*hxxp://4ad23745.dyndns.info/agencept.php?
vialjack=428181*

*hxxp://4ad96968.dyndns.info/agencept.php?vialjack
%3D428181*

*hxxp://4ad21321.dyndns.info/agencept.php?
vialjack=428181*

**The same email (xbroshost@live.com) is also known
to have registered the following phishing domains in
the past:**

hxxp://www.realtorviewproperties.info/realtorjj/index.htm

hxxp://www.usaindependentmerchids.com

hxxp://www.usamerchandiseinc.com/

hxxp://www.blogconsciente.com/ secadmin/eLogin.php

Although the cybercriminal/gang of cybercriminals behind this campaign applied basic OPSEC practices to it,

the fact that the C &C/malicious payload acquisition strategy is largely centralized, (thankfully) indicates a critical flaw in their mode of thinking.

This post has been reproduced from [11]Dancho Danchev's blog. Follow him [12]on Twitter.

79

1. <http://ddanchev.blogspot.com/2013/02/dissecting-nbcs-exploits-and-malware.html>
2. http://en.wikipedia.org/wiki/Late_Night_with_Jimmy_Fallon
3. <http://www.google.com/interstitial?url=http://www.latenightwithjimmyfallon.com/>
4. <http://www.google.com/safebrowsing/diagnostic?site=20-monkeys-b.com/&hl=en>
5. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0431>
6. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1723>
7. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0188>
8. <https://www.virustotal.com/en/file/3a85fdd707f3d040e1e92bc73b9ac5c202f69923821e1405039bc95b80e13033/analysis>

[is/1362605170/](#)

9.

[https://www.virustotal.com/en/file/0a99152fd0788f0bb9ddbda27fc30aa2f924e96aeeb82dc8f8a0d9e4a1eafa34/analysis](https://www.virustotal.com/en/file/0a99152fd0788f0bb9ddbda27fc30aa2f924e96aeeb82dc8f8a0d9e4a1eafa34/analysis/1362605222/)

[is/1362605222/](#)

10.

[https://www.virustotal.com/en/file/11e02cf5c9ec18e0bba7c17ca83ce2e4c8672a810a3da1bf35f15ba014f5b647/analysis](https://www.virustotal.com/en/file/11e02cf5c9ec18e0bba7c17ca83ce2e4c8672a810a3da1bf35f15ba014f5b647/analysis/1362605408/)

[is/1362605408/](#)

11. <http://ddanchev.blogspot.com/>

12. <http://twitter.com/danchodanchev>

80



Dissecting NBC's Late Night with Jimmy Fallon Web Site Compromise (2013-03-07 00:52)

[1]Oops, they did it again!

The official Web site (

hxxp://www.latenightwithjimmyfallon.com) of

[2]NBC's Late Night With Jimmy Fallon is currently

[3]compromised/hacked and is automatically serving

multiple Java exploits to its visitors through a tiny iFrame

element embedded on the front page. According to

[4]Google's Safe Browsing Diagnostic page, the same

malicious iFrame domain that affected the Web site, is also known to have affected 15 more domains.

Let's dissect the campaign, expose the complete domains portfolio used in the campaign, reproduce the malicious payload, and establish a direct connection between this campaign, and a series of phishing campaigns that appear to have been launched by the same cybercriminal/gang of cybercriminals.

Sample

client-side

exploitation

chain:

*hxxp://20-monkeys-b.com/exp/agencept.php?
vialjack=339214*

-

144.135.8.182; 192.154.103.66 -> hxxp://20-monkeys-b.com/exp/tionjett.php

Although the currently embedded iFrame domain is offline, we know that on 2013-03-06 17:02:35 it used to

respond to 192.154.103.66. We've got several malicious domains currently parked at the same IP and respon-

ing, allowing us to obtain the malicious payload used in the campaign affecting NBC's Web site. Upon further

examination, the obtained malicious PDF used in the campaign, also attempts to connect to the initial iFrame do-

main (**20-monkeys-b.com**), proving that the domains are operated by the same cybercriminal/gang of cybercriminals.

Sample exploitation chain for a currently active malicious domain responding to 192.154.103.66:

hxxp://poople-

81

*huelytics.com/exp/agencept.php?vialjack=694842 ->
hxxp://poople-huelytics.com/exp/addajapa/jurylamp.jar ->
hxxp://poople-huelytics.com/exp/addajapa/ptlyable.jar ->
hxxp://poople-huelytics.com/exp/jectrger.php*

Sample client-side exploits served: [5] *CVE-2013-0431*;
[6] *CVE-2012-1723*; [7] *CVE-2010-0188*

Sample detection rates for the reproduced malicious payload:

test.pdf - [8]**MD5:**

013ed8ef6d92cfe337d9d82767f778da - detected by 10 out of 46 antivirus scanners as

PDF:Exploit.PDF-JS.VU

jurylamp.jar - [9]**MD5:**

dcba86395938737b058299b8e22b6d65 - detected by 7 out of 46 antivirus scanners as

Exploit:Java/CVE-2013-0431

ptlyable.jar - [10]**MD5:**

2446aa6594fc7935ca13b130d4f67442 - detected by 6 out of 46 antivirus scanners as

HEUR:Exploit.Java.CVE-2012-1723.gen

test.pdf drops **MD5:**
51311FDECCD8B6BC5059BE33E0046A27 and **MD5:**
72B670F4582BC73C0D05FF506B51B8EB it

then attempts to obtain the malicious payload from **20-monkeys-b.com/exp/senccute.php?** (144.135.8.182)

Responding to 192.154.103.66 are also the following malicious domains:

snova-vdel-e.com

mimemimikat.info

Malicious domain names reconnaissance:

20-monkeys-b.com - Email: haneslyndsey@yahoo.com

poople-huelytics.com - Email: brianmyhalyk@yahoo.com

snova-vdel-e.com - Email: guerin_k@yahoo.com

mimemimikat.info - Email: xbroshost@live.com

More domains share the same exploitation directory structure (agencept.php?vialjack=) such as for instance:

*hxxp://upd.pes2020.com.ar/up/agencept.php?vialjack
%3D219215*

*hxxp://upd.typescript.com.ar/up/agencept.php?
vialjack=219215*

*hxxp://4ad32203.dyndns.info/agencept.php?
vialjack=428181*

*hxxp://4ad34364.dyndns.info/agencept.php?
vialjack=428181*

*hxxp://4ad28306.dyndns.info/agencept.php?
vialjack=428181*

*hxxp://4ad23745.dyndns.info/agencept.php?
vialjack=428181*

*hxxp://4ad96968.dyndns.info/agencept.php?vialjack
%3D428181*

*hxxp://4ad21321.dyndns.info/agencept.php?
vialjack=428181*

The same email (xbroshost@live.com) is also known to have registered the following phishing domains in

the past:

hxxp://www.realtorviewproperties.info/realtorjj/index.htm

hxxp://www.usaindependentmerchids.com

hxxp://www.usamerchandiseinc.com/

hxxp://www.blogconsciente.com/ secadmin/eLogin.php

Although the cybercriminal/gang of cybercriminals behind this campaign applied basic OPSEC practices to it,

the fact that the C &C/malicious payload acquisition strategy is largely centralized, (thankfully) indicates a critical flaw in their mode of thinking.

1. <http://ddanchev.blogspot.com/2013/02/dissecting-nbcs-exploits-and-malware.html>

2.

http://en.wikipedia.org/wiki/Late_Night_with_Jimmy_Fallon

3. [http://www.google.com/interstitial?](http://www.google.com/interstitial?url=http://www.latenightwithjimmyfallon.com/)

[url=http://www.latenightwithjimmyfallon.com/](http://www.latenightwithjimmyfallon.com/)

82

4. <http://www.google.com/safebrowsing/diagnostic?site=20-monkeys-b.com/&hl=en>

5. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0431>

6. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1723>

7. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0188>

8.

[https://www.virustotal.com/en/file/3a85fdd707f3d040e1e92bc73b9ac5c202f69923821e1405039bc95b80e13033/analysis/](https://www.virustotal.com/en/file/3a85fdd707f3d040e1e92bc73b9ac5c202f69923821e1405039bc95b80e13033/analysis/1362605170/)

[1362605170/](https://www.virustotal.com/en/file/3a85fdd707f3d040e1e92bc73b9ac5c202f69923821e1405039bc95b80e13033/analysis/1362605170/)

9.

[https://www.virustotal.com/en/file/0a99152fd0788f0bb9ddbda27fc30aa2f924e96aeeb82dc8f8a0d9e4a1eafa34/analysis/](https://www.virustotal.com/en/file/0a99152fd0788f0bb9ddbda27fc30aa2f924e96aeeb82dc8f8a0d9e4a1eafa34/analysis/1362605222/)

[1362605222/](https://www.virustotal.com/en/file/0a99152fd0788f0bb9ddbda27fc30aa2f924e96aeeb82dc8f8a0d9e4a1eafa34/analysis/1362605222/)

10.

[https://www.virustotal.com/en/file/11e02cf5c9ec18e0bba7c17ca83ce2e4c8672a810a3da1bf35f15ba014f5b647/analysis/](https://www.virustotal.com/en/file/11e02cf5c9ec18e0bba7c17ca83ce2e4c8672a810a3da1bf35f15ba014f5b647/analysis/1362605408/)

[1362605408/](https://www.virustotal.com/en/file/11e02cf5c9ec18e0bba7c17ca83ce2e4c8672a810a3da1bf35f15ba014f5b647/analysis/1362605408/)

83

1.4

April

84



Summarizing Webroot's Threat Blog Posts for March (2013-04-01 21:37)

The following is a brief summary of all of my posts at Webroot's Threat Blog for March, 2013. You can subscribe to

[1]**Webroot's Threat Blog RSS Feed**, or follow me on Twitter:

01. [2]New DIY IRC-based DDoS bot spotted in the wild

02. [3]Cybercriminals release new Java exploits centered exploit kit

03. [4]Segmented Russian "spam leads" offered for sale

04. [5]New DIY hacked email account content grabbing tool facilitates cyber espionage on a mass scale

05. [6]New DIY unsigned malicious Java applet generating tool spotted in the wild

06. [7]Commercial Steam 'information harvester/mass group inviter' could lead to targeted fraudulent campaigns

07. [8]Fake BofA CashPro 'Online Digital Certificate' themed emails lead to malware

- 08.** [9]Spamvertised BBB ‘Your Accreditation Terminated’ themed emails lead to Black Hole Exploit Kit
- 09.** [10]New ZeuS source code based rootkit available for purchase on the underground market
- 10.** [11]Cybercriminals resume spamvertising ‘Re: Fwd: Wire Transfer’ themed emails, serve client-side exploits and malware
- 11.** [12]Cybercrime-friendly community branded HTTP/SMTP based keylogger spotted in the wild
- 12.** [13]Hacked PCs as ‘anonymization stepping-stones’ service operates in the open since 2004
- 13.** [14]Fake ‘CNN Breaking News Alerts’ themed emails lead to Black Hole Exploit Kit
- 14.** [15]Spotted: cybercriminals working on new Western Union based ‘money mule management’ script
- 15.** [16]Malicious ‘BBC Daily Email’ Cyprus bailout themed emails lead to Black Hole Exploit Kit
- 16.** [17]‘ADP Payroll Invoice’ themed emails lead to malware
- 17.** [18]‘Terminated Wire Transfer Notification/ACH File ID’ themed malicious campaigns lead to Black Hole Exploit Kit
- 18.** [19]New DIY RDP-based botnet generating tool leaks in the wild

19. [20]A peek inside the EgyPack Web malware exploitation kit

This post has been reproduced from [21]Dancho Danchev's blog. Follow him [22]on Twitter.

85

1. <http://feeds2.feedburner.com/WebrootThreatBlog>
2. <http://blog.webroot.com/2013/03/04/new-diy-irc-based-ddos-bot-spotted-in-the-wild/>
3. <http://blog.webroot.com/2013/03/05/cybercriminals-release-new-java-exploits-centered-exploit-kit/>
4. <http://blog.webroot.com/2013/03/06/segmented-russian-spam-leads-offered-for-sale/>
5. <http://blog.webroot.com/2013/03/07/new-diy-hacked-email-account-content-grabbing-tool-facilitates-cyber-e-spionage-on-a-mass-scale/>
6. <http://blog.webroot.com/2013/03/08/new-diy-unsigned-malicious-java-applet-generating-tool-spotted-in-the-wild/>
7. <http://blog.webroot.com/2013/03/11/commercial-steam-information-harvester-mass-group-inviter-could-lead-to-targeted-fraudulent-campaigns/>
8. <http://blog.webroot.com/2013/03/12/fake-bofa-cashpro-online-digital-certificate-themed-emails-lead-to-malware/>

9. <http://blog.webroot.com/2013/03/13/spamvertised-bbb-your-accreditation-terminated-themed-emails-lead-to-black-hole-exploit-kit/>

10.

<http://blog.webroot.com/2013/03/14/new-zeus-source-code-based-rootkit-available-for-purchase-on-the-underground-market/>

11. <http://blog.webroot.com/2013/03/15/cybercriminals-resume-spamvertising-re-fwd-wire-transfer-themed-emails-serve-client-side-exploits-and-malware/>

12. <http://blog.webroot.com/2013/03/19/cybercrime-friendly-community-branded-httpsmtp-based-keylogger-spotted-in-the-wild/>

13. <http://blog.webroot.com/2013/03/20/hacked-pcs-as-anonymization-stepping-stones-service-operations-in-the-open-since-2004/>

14.

<http://blog.webroot.com/2013/03/21/fake-cnn-breaking-news-alerts-themed-emails-lead-to-black-hole-exploit-kit/>

15. <http://blog.webroot.com/2013/03/22/spotted-cybercriminals-working-on-new-western-union-based-money-mule-m>

[anagement-script/](#)

16.

[http://blog.webroot.com/2013/03/25/malicious-bbc-daily-email-cyprus-bailout-themed-emails-lead-to-black](http://blog.webroot.com/2013/03/25/malicious-bbc-daily-email-cyprus-bailout-themed-emails-lead-to-black-hole-exploit-kit/)

[-hole-exploit-kit/](#)

17. <http://blog.webroot.com/2013/03/26/adp-payroll-invoice-themed-emails-lead-to-malware/>

18. <http://blog.webroot.com/2013/03/27/terminated-wire-transfer-notificationach-file-id-themed-malicious-campaigns-lead-to-black-hole-exploit-kit/>

[aigns-lead-to-black-hole-exploit-kit/](#)

19. <http://blog.webroot.com/2013/03/28/new-diy-rdp-based-botnet-generating-tool-leaks-in-the-wild/>

20. <http://blog.webroot.com/2013/03/29/a-peek-inside-the-egypt-pack-web-malware-exploitation-kit/>

21. <http://ddanchev.blogspot.com/>

22. <http://twitter.com/danchodanchev>

86



Historical OSINT - The "BadB International" Cybercrime Enterprise (2013-04-10 21:53)

[1]BadB is the nickname of Vladislav Anatolievich Horohorin, a high profile carder, who eventually **[2]got busted in France in 2010**. This month, he was

[3]**sentenced to serve 88 months in prison**, ordered to pay \$125,739 in

restitution, and sentenced to two years of supervised release.

In the wake of these events, I decided to release some raw OSINT data regarding BadB's official Web site,

hxxp://badb.biz.

87



Related URLs: *hxxp://badb.biz; hxxp://badb.org; hxxp://dumps.name*

Emails:

badb4cc@yahoo.com;

metaksa_s@yahoo.com;

support@agava.com;

admin@agava.com;

ad-

min@carderplanet.biz

ICQ: 49162552

Phone number: +19522325532 (Working according to BadB in 2009)

IP hosting history for badb.biz from 2005 to 2010 in the format (initial hosting IP -> IP change detected

to a

new IP):

217.107.212.115 -> 64.202.167.129

64.202.167.129 -> 217.107.212.115

217.107.212.115 -> 217.107.212.9

217.107.212.9 -> 89.108.66.104

89.108.66.104 -> 68.178.232.99

68.178.232.99 -> 89.108.66.104

88



216.8.177.23 -> 78.109.18.150

78.109.18.150 -> 196.32.222.9

89.108.73.117 - > 94.75.221.75

94.75.221.75 -> 92.241.164.92

Sample About Us section description from badb.biz:

We are independent e-commerce security investigation group. We are help e-commerce organisations such as Visa,

Mastercard, regional processings and other e-commerce structures to understand how vulnerable they are. We are

not connected to any criminal structures, not performing any outlaw actions by ourselves, not selling drugs, not

sendind any spam, not connected to any child porno, not supporting terrorists themselves nor terrorist organisations.

If you received any spam from us - this is a fake of our enemies we are never use spam to promote our site. All

information you can read here provided "As Is" and only for educational purposes. All articles are copyrighted. If you 89

wish to take any part of information from here - please refer to origination site. All we do - is we have for sale some dumps, cvvs and cobs - just for experemental purposes of our custommers ;-) We listen and effectively respond to your

needs and those of your clients. We are experts at translating those needs into marketing solutions that work, look

great and communicate well. Each day brings increased opportunity to increase business in current as well as new.

This case is a great example of a simple fact - with or without BadB, [4]**the market for stolen credit cards**

data, continued growing throughout the entire 2011.

Then in 2012, we witnessed two law enforcement operations,

courtesy of [5]**SOCA**, and the [6]**FBI**. However, despite these efforts, the market for stolen credit cards data remains as vibrant as always.

Thanks to the [7]**standardization taking place in respect to the money mule recruitment process**, as well as

the nearly identical online shops for stolen credit cards data, those who cannot "cash out" the balances of the credit cards, will choose to [8]**risk-forward** the selling process to the buyers of the stolen data. The rest, will basically continue looking for more efficient, automatic, and anonymous ways to get access to the stolen money, continuing

to rely on money mules of virtual currencies.

This post has been reproduced from [9]Dancho Danchev's blog. Follow him [10]on Twitter.

1. <http://www.youtube.com/watch?v=9y4ijOXGeg>
2. <http://www.wired.com/threatlevel/2010/08/badb/>
3. <http://www.justice.gov/opa/pr/2013/April/13-crm-386.html>
4. <http://ddanchev.blogspot.com/2011/10/exposing-market-for-stolen-credit-cards.html>
5. <http://www.soca.gov.uk/news/446-web-domains-seized-in-international-operation-to-target-online-fraudsters>
6. <http://www.zdnet.com/blog/security/24-cybercriminals-arrested-in-operation-card-shop/12435>
7. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>
8. <http://blog.webroot.com/2013/03/22/spotted-cybercriminals-working-on-new-western-union-based-money-mule-management-script/>

9. <http://ddanchev.blogspot.com/>

10. <http://twitter.com/danchodanchev>

90



Historical OSINT - The "BadB International" Cybercrime Enterprise (2013-04-10 21:53)

[1]**BadB is the nickname of Vladislav Anatolievich Horohorin**, a high profile carder, who eventually [2]**got busted in France in 2010**. This month, he was [3]**sentenced to serve 88 months in prison**, ordered to pay \$125,739 in

restitution, and sentenced to two years of supervised release.

In the wake of these events, I decided to release some raw OSINT data regarding BadB's official Web site,

hxxp://badb.biz.

91



Related URLs: *hxxp://badb.biz; hxxp://badb.org;
hxxp://dumps.name*

Emails:

badb4cc@yahoo.com;

metaksa_s@yahoo.com;

support@agava.com;

admin@agava.com;

ad-

min@carderplanet.biz

ICQ: 49162552

Phone number: +19522325532 (Working according to BadB in 2009)

IP hosting history for badb.biz from 2005 to 2010 in the format (initial hosting IP -> IP change detected to a

new IP):

217.107.212.115 -> 64.202.167.129

64.202.167.129 -> 217.107.212.115

217.107.212.115 -> 217.107.212.9

217.107.212.9 -> 89.108.66.104

89.108.66.104 -> 68.178.232.99

68.178.232.99 -> 89.108.66.104

92



216.8.177.23 -> 78.109.18.150

78.109.18.150 -> 196.32.222.9

89.108.73.117 - >94.75.221.75

94.75.221.75 -> 92.241.164.92

Sample About Us section description from badb.biz:

We are independent e-commerce security investigation group. We are help e-commerce organisations such as Visa,

Mastercard, regional processings and other e-commerce structures to understand how vulnerable they are. We are

not connected to any criminal structures, not performing any outlaw actions by ourselves, not selling drugs, not

sendind any spam, not connected to any child porno, not supporting terrorists itselfes nor terrorist organisations.

If you received any spam from us - this is a fake of our enemies we are never use spam to promote our site. All

information you can read here provided "As Is" and only for educational purposes. All articles are copyrighted. If you 93

wish to take any part of information from here - please reffer to origination site. All we do - is we have for sale some dumps, cvvs and cobs - just for experemental purposes of our custommers ;-) We listen and effectively respond to your

needs and those of your clients. We are experts at translating those needs into marketing solutions that work, look

great and communicate well. Each day brings increased opportunity to increase business in current as well as new.

This case is a great example of a simple fact - with or without BadB, [4]**the market for stolen credit cards**

data, continued growing throughout the entire 2011.

Then in 2012, we witnessed two law enforcement operations,

courtesy of [5]**SOCA**, and the [6]**FBI**. However, despite these efforts, the market for stolen credit cards data remains as vibrant as always.

Thanks to the [7]**standardization taking place in respect to the money mule recruitment process**, as well as

the nearly identical online shops for stolen credit cards data, those who cannot "cash out" the balances of the credit cards, will choose to [8]**risk-forward** the selling process to the buyers of the stolen data. The rest, will basically continue looking for more efficient, automatic, and anonymous ways to get access to the stolen money, continuing

to rely on money mules of virtual currencies.

1. <http://www.youtube.com/watch?v=9y4iijOXGeg>
2. <http://www.wired.com/threatlevel/2010/08/badb/>
3. <http://www.justice.gov/opa/pr/2013/April/13-crm-386.html>
4. <http://ddanchev.blogspot.com/2011/10/exposing-market-for-stolen-credit-cards.html>
5. <http://www.soca.gov.uk/news/446-web-domains-seized-in-international-operation-to-target-online-fraudsters>

6. <http://www.zdnet.com/blog/security/24-cybercriminals-arrested-in-operation-card-shop/12435>

7. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>

8. [http://blog.webroot.com/2013/03/22/spotted-cybercriminals-working-on-new-western-union-based-money-mule-m](http://blog.webroot.com/2013/03/22/spotted-cybercriminals-working-on-new-western-union-based-money-mule-management-script/)

[anagement-script/](#)

94



What's the ROI on Going to a Virtual Blackhat SEO School? (2013-04-17 23:45)

For years, fraudulent or **[1]purely malicious actors** have been abusing the online advertising market, by **[2]directly hijacking** and redirecting **[3]the revenue flow**, or by **[4]successfully and efficiently** hijacking as much percentage of legitimate search traffic as possible, and monetizing it through the use of **[5]blackhat SEO (search engine**

optimization) tactics/shady affiliate networks.

[6]Monetizing the very monetization process?

Standardizing the revenue generation, and knowledge spreading

streams, achieving efficiencies in the process, and directly contributing to a new, this time better trained/educated

generation of Blackhat SEO-ers? Someone he's knowingly or unknowingly on a mission. A mission with a brand.

In this post, I'll profile a highly successful [7]**blackhat SEO** 'school' that promises the Moon, but asks for nothing except \$1,000 for the training course, which will turn you into a sophisticated blackhat SEO expert, netting you huge amounts of money.

Operating in the open since 2010, the service is currently (2013) asking for \$350, presumably to keep the new

customers flow going. Since it's initial launch data, the business model has been relying on a loyal set of people who

already "took" the course, and continue making money up to present day. A loyalty and happy customer "feedback"

best demonstrated by featuring exclusive screenshots courtesy of the happy customers.

Initial forum advertisement:

95

Welcome to the forum millionaires! So, I decided, now I will welcome the new students.

And you know why?

My course, and our forum for more than two years, and during that time has accumulated a huge pile of re-

views with the statistics. Wondered how many of my students have earned over 2 years on my course?

And it turned out that except cars, apartments, purely according to PP, pupils together earned 17 million rubles! And

it is only those who have shown their statistics. And I think in 2 years they could make a few more millions. (Figure

is slightly inaccurate to 9 lines in a notebook I got tired and started to round + decided not to take into account the 3,000,000 earnings per pupil)

In two years, we have made dozens of millionaires in Russia, Ukraine and Belarus Their lives changed immedi-

ately, as soon as they hit the family. People sitting in debt in a few months to buy a new car.

People are sitting at their desks yesterday brought home two monthly salaries parents, and explained that it is

unashamedly from the Internet, it is their earnings!

People who are already my course have been very successful become even more successful. The forum is sta-

ble enough people who earn a day 50-60 thousand rubles. This is not theoretical, not uncle in suits, this is the same young guys like you or me.

Although I must admit, the forum is and uncle in suits for 30-40 years, primarily to get through doorways capital to support their business.

And all these people realize that they are family, friends, and they willingly associate, dividing their experi-

ences, secrets! Access to the course - it is a unique opportunity to touch the thought of successful people, to breathe the same air with them, get their energy and join the ranks of millionaires.

As early as the year, the forum has two tech support, and username, people are few easy counseled hundreds

of students and even if they did not do dory - would know what the perfect doorway.

BUT! They do work, make Dora always advise how to make your doorway even better answer the most stupid

question, and will lead to the most stable earnings.

Now, if you are reading these lines and think that \$ 1000 for access and the opportunity to become a million-

aire in 24\7 support from a support, for the opportunity to be in the new family is expensive, I never selling you access.

We need people who value themselves, their money and time. If \$ 1,000 seems to you a great price, then you

will never become a millionaire from the internet and you simply do not want my family.

Imagine you paid \$ 1,000 in the bank say, come back every day to ask questions and get a month - \$ 100,000,

it is tempting? Here's a bank - this is our forum. And 80 pages of reviews stands surety for this bank.

You may think, but what for me is all good topic no one will sell!

And I grieve you, it's not the topic, not the scheme, not the holy grail, it's work. Work by a support forum and

make it so simple that you will forget the times when you have not worked with doorways.

A successful guys will charge you so much energy that the work will be for you the best thing in life. You're going to sleep at 4:00, waking up in the middle of the night with burning eyes, watch as your dorveychiki live there, and how

96

many thousands have already dripped while you were sleeping.

Through it all the disciples, and I think they would give, and 10 and 100 thousand dollars to get through it again.

But there is a dump in a Public Forum, everything is - you say.

And I'll tell you the story of how one day I lost the backup of offline and restored the forum 15 minutes ago

from what it was last time. And it was a huge mistake! Lost about 50 messages, 12 topics and 5-6 blog posts! The

disciples were indignant. On our forum mad update rate, and dump the last year and the relevance of information

out there already in negative degrees and I am afraid that only harms doorways.

But I can learn myself! Yes you can, spend a few years on independent learning.

And you can put a time out and spend \$ 1000 on an active training week and immediately makes the door-

ways correctly. Once again, we are waiting for our club anonymous millionaires of people who know the value of

money and his own time, who want to invest in yourself, earn, and not break your head against the wall, when there are people who will show how to get around.

Course can be purchased on the preliminary interview in ICQ price - \$ 1000.

And remember, we are, we need special people, very few of them, they are people who are willing to invest in

yourself and do not try to save yourself cheaply though. So I throw in ICQ to ignore anyone who asks me for a discount or credit. I understand that in spite of the 80-page review, you may be unsure if it will work with you. Therefore, we give a new guarantee manibeka. If two weeks you feel - that doorway - it's not yours, we will refund the money and

pay the top 5 million rubles, for what you have spent your time!

Frequently Asked Questions (FAQ)

Good day, and now its time to answer all the questions a novice who wants to buy a course to dot the i, made to

understand that he buys, he will get what may dobitsya.Nus's begin.

1.Chem we do?

Black seo.Dorvei.Dory are very flexible and tenacious tool for earnings, its flexibility due to the variety of topics

and types of monetization, and vitality - the existence of PS, and how long will exist as long as the search engines

will be using dory. We produce traffic, ie the users, ie the people, the traffic is the blood in the veins of the internet, and this is the main advantage that dorveyschik unlike white SEOs can in a short time to break a lot more traffa a

completely different subjects and to merge it back where it needs . in a simple version of all is:

1.Registriruemsya an affiliate program, it gives you the choice of partner sites of some topics (topics vary from porn and finishing all kinds of divination), statistics (to track kollvo coming to your site, paid for kollvo, Colva who have come again).

2.Delaem doorway, we find:

- Thematic traffistye quality keys (which are appropriate to the site subject we took from PP)

- Template

- Text

All this is described in detail in the course and on the forum.

3.Zalivaem doorway to shell

4.Zhdem 4.3 apa (an - update Yandex search results, also known as SERP, quite by chance, usually up to one week, sometimes more)

5.Poluchaem traff and accordingly money.

Well this is just a simple and obvious option, work with SMS affiliate, to start - the fact that many small minded people to talk about the thousandth time of death doorways as

income, just because of the changes in the SMS payment, it's

97

wrong, it's stupid, it's self-deception to deceive drugih. I as, say, we have learned to produce traffic, our traffic started to give Dora and now we have to redirect it somewhere ie merge and convert / convert into money, a lot of options:

1.Partnerki with sms payment, the most obvious and as I wrote the best option to start.

2.Partnerki pay-per-download and install the file, such PP a lot, and they are all different, from the fact that you are paying for the jump and the malicious Trojan or whether something like that, to quite formal type of games WORLD

of-tanks, Yandex bars etc. and tp.Imeya large amounts of traffic (which is the second task dorveyschika, increase the volume of traffic) in the first and in the second option holders PP will take you with open arms and make bonuses.

3.Svoi online shopping and platniki.V this topic a little feedback from these guys, as many prefer to work with SMS

and other PP, but byvali.Odin met some of the students at comrade serche, he did an Internet jewelry store and the

problem was my student in the production of traffic, he quickly picked up, done and grabbed a piece of the profit.

All that I wrote just for you to understand, I teach mine traffic, targeted traffic from search engines, I would suggest the best methods of monetization, by which usually fight off the course, but never forget that you have a great

opportunity to go and grab a piece of the traffic on desired topics with Yandex and merge where necessary.

2. Naverhoe topic died, bought her so much, so long existed, much is competition?

I am for all the time of sale of the course has experienced the death of a thousand and one as the reward

scheme, but that's amazing, for some reason all those who want to - successfully earn dorah. Chto for competition -

in dorah very high turnover, namely Dora always fly into the index (Yandex search) and flew over, it's all backed by

the characteristic features of the behavior dorveyschika and dorveyschik often tasting dough, he realized how easily

make dory, does pack and walk yourself getting denyuzhki, leaving room for other results.

3. Zachem you sell?

That's what I do - called infobiznesom admit, when all this started, I such a word and znal. Est two concepts,

with which you can ever accurately explain the infobiznesa, information and insider information autsayder. Kogda-

long ago, when I was dramas and gathering information about them bit by bit on various forums - I was an outsider,

I was not available methods that can quickly lead to success, and everything had to be found by experiment, my first

income from went after 3 months and a naked enthusiasm nadezhdy. Pokupaya course you get insider information,

which is called the bat, straight to the kitchen where everything is cooked, I do not sell super flow sheet, I only give an opportunity and take it for a fee, sell their time and, in recent years, more and more nerves, which is why, in order to maintain this non-renewable resource, and I wrote it, do not be lazy, read.

4.Kak guarantee that I Otobaya course?

No! Absolutely! Absolutely no, When we first started selling rate - while I was still able to provide guarantees

to score reviews, to prove to everyone that the theme works, but now - no, no way! Your warranty - you, your desire,

hard work , commitment - that guarantee it, I can not guarantee anything I can not and will not, often when a person

writes me word guarantee, he wants me to take responsibility for his lazy ass over - No, I'm sorry.

5.Malenky advice, how to effectively master the course and see if it fits you at all.

My experience learning heaps different people, still divided them into two types, this is a huge difference, the

gap between the two approaches to learning, results in a huge gap in the success of these students.

The first type: people with pure slave mentality, they need to stick, do not explain, do not need to seek understanding, just poke, push there, click here.

How he thinks: Suppose we make a template for Dora, and we need to write deksripshen, deskripshen - description of the site which comes out at the bottom under the link, his task - to give information about the page and encourage people to move to tyknut ie sayt. On asks me what write here, I explain what it is and I say write something that would please you, and you would make pereyti. On in a stupor, he can not think and can not even offer the option, he just

98

wants me to tell him that there napisat. Eto not right!

The second type: The second type is often trying to organize all the information in the first place to understand how

things work, and there are already having a solid foundation and framework - to batter me with questions and to

increase their knowledge, for example of the first type, the second type, after hearing deskripshen what and why it is, would compare with my examples and offered his variant. Vot so you have to be, if you're so - I'll be glad to have you

in the ranks of students.

6. Tsena huge! Tc asshole, the course did not buy, but it's an asshole! Reviews delete it!

Do not like the price - do not buy it, no one vparivaet, there is no hint of the imposition of the course, under

the gun more so no one makes pokupat. Golye hit and conclusions about the course of those who did not buy it -

please do not post, I immediately call the moderators, all is removed, how can you talk about the course, not having

been on FSU How we can talk about what you do not know, if you were not in the motivation section on the forum

where dozens of success stories of students? I bought the course, learned, wrote otzyv. Ya a moderator section only

CEO and section on "Work" where this topic - I can not moderate.

7. What I receive after payment?

Education - after payment receive video / txt + access to the forum, watch / read / do, have questions - ask,

discuss - send to the forum, no - rasskazyvayu. Esli you read the topic that many people write that the chip in

the forum, unnecessarily there is a lot of relevant info and all you happy pomoch. Ves free software data - paid

counterparts shown in forume. Dostup forum and consultations Asik - unlimited.

8. Skolko need to successfully quick Start?

Then (in a week or another) will need \$ 10-20 for vpn (both analog proxy / socks or Dedicated Server) and

200-300 rubles for glanders.

9. Kak Otobaya fast I / osvoyu course?

Everything is individual, calculate and even about to say (to you) this time period may depend both on the

human factor (your knowledge, experience) and on Yandex, which is quite nepredskazuem. Osnovyvayas on the

experience of previous students gives dor \$ 200 4 up to 30 days after the publication of indeks. 3-4 apa usually climbs Dor ups are completely random, look here <http://seobudget.ru/updates> labeled SERP.

10. Rynok forum.

In our forum, which you can access after purchase - there is a market, as in any other forum, it is an integral

part of the forum who wants to live, and in the end we are all in this forum for one reason - we all want to make

money someone else has earned, someone just nachinaet. V Unlike other forums - the market for FSU controlling me,

he monopolizirovan. Kursy of its kind in the forum - I only sell and no other, their commercial activities in the forum -

with me coordinate is not necessary, but if it is removed - so she does not belong here.

Screenshots provided by actual customers of the service, featuring its primary ICQ contact point:

99



100



101



102



103



104



105



106



107



108



109



110



111



112



113



114



115



116



117



118



Blackhat SEO - it doesn't just pay the bills.

This post has been reproduced from [8]Dancho Danchev's blog. Follow him [9]on Twitter.

1. http://www.av-test.org/fileadmin/pdf/avtest_2013-03_search_engines_malware_english.pdf

2. <http://ddanchev.blogspot.com/2010/07/sampling-malicious-activity-inside.html>
3. <http://www.zdnet.com/blog/security/cybercriminals-promoting-malware-friendly-search-engines/3333>
4. <http://www.zdnet.com/blog/security/botnets-committing-click-fraud-observed/1200>
5. https://www.google.com/#output=search&sclient=psy-ab&q=site:ddanchev.blogspot.com+%22blackhat+seo%22&oq=site:ddanchev.blogspot.com+%22blackhat+seo%22&gs_l=
6. <http://ddanchev.blogspot.com/2009/06/peek-inside-managed-blackhat-seo.html>
7. <https://www.google.com/#output=search&sclient=psy-ab&q=site:ddanchev.blogspot.com+blackhat+seo>
8. <http://ddanchev.blogspot.com/>
9. <http://twitter.com/danchodanchev>

119



What's the ROI on Going to a Virtual Blackhat SEO School? (2013-04-17 23:45)

For years, fraudulent or **[1]purely malicious actors** have been abusing the online advertising market, by **[2]directly hijacking** and redirecting **[3]the revenue flow**, or by **[4]successfully and efficiently** hijacking as much percentage of legitimate search traffic as possible, and

monetizing it through the use of [5]**blackhat SEO (search engine**

optimization) tactics/shady affiliate networks.

[6]**Monetizing the very monetization process?**

Standardizing the revenue generation, and knowledge spreading

streams, achieving efficiencies in the process, and directly contributing to a new, this time better trained/educated

generation of Blackhat SEO-ers? Someone he's knowingly or unknowingly on a mission. A mission with a brand.

In this post, I'll profile a highly successful [7]**blackhat SEO 'school'** that promises the Moon, but asks for nothing except \$1,000 for the training course, which will turn you into a sophisticated blackhat SEO expert, netting you

huge amounts of money.

Operating in the open since 2010, the service is currently (2013) asking for \$350, presumably to keep the new

customers flow going. Since it's initial launch data, the business model has been relying on a loyal set of people who

already "took" the course, and continue making money up to present day. A loyalty and happy customer "feedback"

best demonstrated by featuring exclusive screenshots courtesy of the happy customers.

Initial forum advertisement:

Welcome to the forum millionaires! So, I decided, now I will welcome the new students.

And you know why?

My course, and our forum for more than two years, and during that time has accumulated a huge pile of re-

views with the statistics. Wondered how many of my students have earned over 2 years on my course?

And it turned out that except cars, apartments, purely according to PP, pupils together earned 17 million rubles! And

it is only those who have shown their statistics. And I think in 2 years they could make a few more millions. (Figure

is slightly inaccurate to 9 lines in a notebook I got tired and started to round + decided not to take into account the 3,000,000 earnings per pupil)

In two years, we have made dozens of millionaires in Russia, Ukraine and Belarus Their lives changed immedi-

ately, as soon as they hit the family. People sitting in debt in a few months to buy a new car.

People are sitting at their desks yesterday brought home two monthly salaries parents, and explained that it is

unashamedly from the Internet, it is their earnings!

People who are already my course have been very successful become even more successful. The forum is sta-

ble enough people who earn a day 50-60 thousand rubles. This is not theoretical, not uncle in suits, this is the same

young guys like you or me.

Although I must admit, the forum is and uncle in suits for 30-40 years, primarily to get through doorways capital to support their business.

And all these people realize that they are family, friends, and they willingly associate, dividing their experi-

ences, secrets! Access to the course - it is a unique opportunity to touch the thought of successful people, to breathe the same air with them, get their energy and join the ranks of millionaires.

As early as the year, the forum has two tech support, and username, people are few easy counseled hundreds

of students and even if they did not do dory - would know what the perfect doorway.

BUT! They do work, make Dora always advise how to make your doorway even better answer the most stupid

question, and will lead to the most stable earnings.

Now, if you are reading these lines and think that \$ 1000 for access and the opportunity to become a million-

aire in 24\7 support from a support, for the opportunity to be in the new family is expensive, I never selling you access.

We need people who value themselves, their money and time. If \$ 1,000 seems to you a great price, then you

will never become a millionaire from the internet and you simply do not want my family.

Imagine you paid \$ 1,000 in the bank say, come back every day to ask questions and get a month - \$ 100,000,

it is tempting? Here's a bank - this is our forum. And 80 pages of reviews stands surety for this bank.

You may think, but what for me is all good topic no one will sell!

And I grieve you, it's not the topic, not the scheme, not the holy grail, it's work. Work by a support forum and

make it so simple that you will forget the times when you have not worked with doorways.

A successful guys will charge you so much energy that the work will be for you the best thing in life. You're going to sleep at 4:00, waking up in the middle of the night with burning eyes, watch as your dorveychiki live there, and how

121

many thousands have already dripped while you were sleeping.

Through it all the disciples, and I think they would give, and 10 and 100 thousand dollars to get through it again.

But there is a dump in a Public Forum, everything is - you say.

And I'll tell you the story of how one day I lost the backup of offline and restored the forum 15 minutes ago

from what it was last time. And it was a huge mistake! Lost about 50 messages, 12 topics and 5-6 blog posts! The

disciples were indignant. On our forum mad update rate, and dump the last year and the relevance of information

out there already in negative degrees and I am afraid that only harms doorways.

But I can learn myself! Yes you can, spend a few years on independent learning.

And you can put a time out and spend \$ 1000 on an active training week and immediately makes the door-

ways correctly. Once again, we are waiting for our club anonymous millionaires of people who know the value of

money and his own time, who want to invest in yourself, earn, and not break your head against the wall, when there

are people who will show how to get around.

Course can be purchased on the preliminary interview in ICQ price - \$ 1000.

And remember, we are, we need special people, very few of them, they are people who are willing to invest in

yourself and do not try to save yourself cheaply though. So I throw in ICQ to ignore anyone who asks me for a discount or credit. I understand that in spite of the 80-page review, you may be unsure if it will work with you. Therefore, we give a new guarantee manibeka. If two weeks you feel - that doorway - it's not yours, we will refund the money and

pay the top 5 million rubles, for what you have spent your time!

Frequently Asked Questions (FAQ)

Good day, and now its time to answer all the questions a novice who wants to buy a course to dot the i, made to

understand that he buys, he will get what may dobitsya.Nus's begin.

1.Chem we do?

Black seo.Dorvei.Dory are very flexible and tenacious tool for earnings, its flexibility due to the variety of topics

and types of monetization, and vitality - the existence of PS, and how long will exist as long as the search engines

will be using dory. We produce traffic, ie the users, ie the people, the traffic is the blood in the veins of the internet, and this is the main advantage that dorveyschik unlike white SEOs can in a short time to break a lot more traffa a

completely different subjects and to merge it back where it needs . in a simple version of all is:

1.Registriruemsya an affiliate program, it gives you the choice of partner sites of some topics (topics vary from porn and finishing all kinds of divination), statistics (to track kollvo coming to your site, paid for kollvo, Colva who have come again).

2.Delaem doorway, we find:

- Thematic traffistye quality keys (which are appropriate to the site subject we took from PP)

- Template

- Text

All this is described in detail in the course and on the forum.

3.Zalivaem doorway to shell

4.Zhdem 4.3 apa (an - update Yandex search results, also known as SERP, quite by chance, usually up to one week, sometimes more)

5.Poluchaem traff and accordingly money.

Well this is just a simple and obvious option, work with SMS affiliate, to start - the fact that many small minded people to talk about the thousandth time of death doorways as income, just because of the changes in the SMS payment, it's

122

wrong, it's stupid, it's self-deception to deceive drugih.I as, say, we have learned to produce traffic, our traffic started to give Dora and now we have to redirect it somewhere ie merge and convert / convert into money, a lot of options:

1.Partnerki with sms payment, the most obvious and as I wrote the best option to start.

2.Partnerki pay-per-download and install the file, such PP a lot, and they are all different, from the fact that you are paying for the jump and the malicious Trojan or whether something like that, to quite formal type of games WORLD

of-tanks, Yandex bars etc. and tp.Imeya large amounts of traffic (which is the second task dorveyschika, increase the volume of traffic) in the first and in the second option holders PP will take you with open arms and make bonuses.

3.Svoi online shopping and platniki.V this topic a little feedback from these guys, as many prefer to work with SMS

and other PP, but byvali.Odin met some of the students at comrade serche, he did an Internet jewelry store and the

problem was my student in the production of traffic, he quickly picked up, done and grabbed a piece of the profit.

All that I wrote just for you to understand, I teach mine traffic, targeted traffic from search engines, I would suggest the best methods of monetization, by which usually fight off the course, but never forget that you have a great

opportunity to go and grab a piece of the traffa on desired topics with Yandex and merge where necessary.

2.Navernoe topic died, bought her so much, so long existed, much is competition?

I am for all the time of sale of the course has experienced the death of a thousand and one as the reward

scheme, but that's amazing, for some reason all those who want to - successfully earn dorah.Chto for competition -

in dorah very high turnover, namely Dora always fly into the index (Yandex search) and flew over, it's all backed by

the characteristic features of the behavior dorveyschika and dorveyschik often tasting dough, he realized how easily

make dory, does pack and walk yourself getting denyuzhki, leaving room for other results.

3.Zachem you sell?

That's what I do - called infobiznesom admit, when all this started, I such a word and znal.Est two concepts,

with which you can ever accurately explain the infobiznesa, information and insider information autsayder.Kogda-

long ago, when I was dramas and gathering information about them bit by bit on various forums - I was an outsider,

I was not available methods that can quickly lead to success, and everything had to be found by experiment, my first

income from went after 3 months and a naked enthusiasm nadezhdy.Pokupaya course you get insider information,

which is called the bat, straight to the kitchen where everything is cooked, I do not sell super flow sheet, I only give an opportunity and take it for a fee, sell their time and, in recent years, more and more nerves, which is why, in order to maintain this non-renewable resource, and I wrote it, do not be lazy, read.

4.Kak guarantee that I Otobaya course?

No! Absolutely! Absolutely no, When we first started selling rate - while I was still able to provide guarantees

to score reviews, to prove to everyone that the theme works, but now - no, no way! Your warranty - you, your desire,

hard work , commitment - that guarantee it, I can not guarantee anything I can not and will not, often when a person

writes me word guarantee, he wants me to take responsibility for his lazy ass over - No, I'm sorry.

5.Malenky advice, how to effectively master the course and see if it fits you at all.

My experience learning heaps different people, still divided them into two types, this is a huge difference, the

gap between the two approaches to learning, results in a huge gap in the success of these students.

The first type: people with pure slave mentality, they need to stick, do not explain, do not need to seek understanding, just poke, push there, click here.

How he thinks: Suppose we make a template for Dora, and we need to write deksripshen, deskripshen - description of

the site which comes out at the bottom under the link, his task - to give information about the page and encourage

people to move to tyknut ie sayt.On asks me what write here, I explain what it is and I say write something that would please you, and you would make pereyti.On in a stupor, he can not think and can not even offer the option, he just

123

wants me to tell him that there napisat.Eto not right!

The second type: The second type is often trying to organize all the information in the first place to understand how

things work, and there are already having a solid foundation and framework - to batter me with questions and to

increase their knowledge, for example of the first type, the second type, after hearing deskripshen what and why it is, would compare with my examples and offered his variant. Vot so you have to be, if you're so - I'll be glad to have you

in the ranks of students.

6. Tsena huge! Tc asshole, the course did not buy, but it's an asshole! Reviews delete it!

Do not like the price - do not buy it, no one vparivaet, there is no hint of the imposition of the course, under

the gun more so no one makes pokupat. Golye hit and conclusions about the course of those who did not buy it -

please do not post, I immediately call the moderators, all is removed, how can you talk about the course, not having

been on FSU How we can talk about what you do not know, if you were not in the motivation section on the forum

where dozens of success stories of students? I bought the course, learned, wrote otzyv. Ya a moderator section only

CEO and section on "Work" where this topic - I can not moderate.

7. What I receive after payment?

Education - after payment receive video / txt + access to the forum, watch / read / do, have questions - ask,

discuss - send to the forum, no - rasskazyvayu. Esli you read the topic that many people write that the chip in

the forum, unnecessarily there is a lot of relevant info and all you happy pomoch. Ves free software data - paid

counterparts shown in forume. Dostup forum and consultations Asik - unlimited.

8. Skolko need to successfully quick Start?

Then (in a week or another) will need \$ 10-20 for vpn (both analog proxy / socks or Dedicated Server) and

200-300 rubles for glanders.

9. Kak Otobaya fast I / osvoyu course?

Everything is individual, calculate and even about to say (to you) this time period may depend both on the

human factor (your knowledge, experience) and on Yandex, which is quite nepredskazuem. Osnovyvayas on the

experience of previous students gives dor \$ 200 4 up to 30 days after the publication of indeks. 3-4 apa usually climbs Dor ups are completely random, look here <http://seobudget.ru/updates> labeled SERP.

10. Rynok forum.

In our forum, which you can access after purchase - there is a market, as in any other forum, it is an integral

part of the forum who wants to live, and in the end we are all in this forum for one reason - we all want to make

*money someone else has earned, someone just nachinaet.V
Unlike other forums - the market for FSU controlling me,*

*he monopolizirovan. Kursy of its kind in the forum - I only
sell and no other, their commercial activities in the forum -*

*with me coordinate is not necessary, but if it is removed - so
she does not belong here.*

**Screenshots provided by actual customers of the
service, featuring its primary ICQ contact point:**

124



125



126



127



128



129



130



131



132



133



134



135



136



137



138



139



140





Updates will be posted as soon as new developments take place.

1. http://www.av-test.org/fileadmin/pdf/avtest_2013-03_search_engines_malware_english.pdf
2. <http://ddanchev.blogspot.com/2010/07/sampling-malicious-activity-inside.html>
3. <http://www.zdnet.com/blog/security/cybercriminals-promoting-malware-friendly-search-engines/3333>
4. <http://www.zdnet.com/blog/security/botnets-committing-click-fraud-observed/1200>
5. https://www.google.com/#output=search&sclient=psy-ab&q=site:ddanchev.blogspot.com+%22blackhat+seo%22&oq=site:ddanchev.blogspot.com+%22blackhat+seo%22&gs_l=te:ddanchev.blogspot.com+%22blackhat+seo%22&gs_l=
6. <http://ddanchev.blogspot.com/2009/06/peek-inside-managed-blackhat-seo.html>

7. <https://www.google.com/#output=search&sclient=psy-ab&q=site:ddanchev.blogspot.com+blackhat+seo>

144

1.5

May

145



Summarizing Webroot's Threat Blog Posts for April (2013-05-01 14:32)

The following is a brief summary of all of my posts at Webroot's Threat Blog for April, 2013. You can subscribe to

[1]**Webroot's Threat Blog RSS Feed**, or follow me on Twitter:

01. [2]DIY Java-based RAT (Remote Access Tool) spotted in the wild

02. [3]Spamadvertised 'Re: Changelog as promised' themed emails lead to malware

03. [4]Cybercrime-friendly service offers access to tens of thousands of compromised accounts

04. [5]Madi/Mahdi/Flashback OS X connected malware spreading through Skype

05. [6]Cybercriminals selling valid 'business card' data of company executives across multiple verticals

- 06.** [7]A peek inside the 'Zerokit/0kit/ring0 bundle' bootkit
- 07.** [8]DIY Skype ring flooder offered for sale
- 08.** [9]Spamvertised 'Your order for helicopter for the weekend' themed emails lead to malware
- 09.** [10]A peek inside a 'life cycle aware' underground market ad for a private keylogger
- 10.** [11]American Airlines 'You can download your ticket' themed emails lead to malware
- 11.** [12]Cybercriminals offer spam-friendly SMTP servers for rent
- 12.** [13]How mobile spammers verify the validity of harvested phone numbers – part two
- 13.** [14]A peek inside a (cracked) commercially available RAT (Remote Access Tool)
- 14.** [15]DIY Russian mobile number harvesting tool spotted in the wild
- 15.** [16]DIY SIP-based TDoS tool/number validity checker offered for sale
- 16.** [17]CAPTCHA-solving Russian email account registration tool helps facilitate cybercrime
- 17.** [18]Historical OSINT – The 'Boston Marathon explosion' and 'Fertilizer plant explosion in Texas' themed malware 146 campaigns
- 18.** [19]Fake 'DHL Delivery Report' themed emails lead to malware

19. [20]Cybercriminals impersonate Bank of America (BofA), serve malware

20. [21]How fraudulent blackhat SEO monetizers apply Quality Assurance (QA) to their DIY doorway generators

21. [22]Managed 'Russian ransomware' as a service spotted in the wild

This post has been reproduced from [23]Dancho Danchev's blog. Follow him [24]on Twitter.

1. <http://feeds2.feedburner.com/WebrootThreatBlog>
2. <http://blog.webroot.com/2013/04/01/diy-java-based-rat-remote-access-tool-spotted-in-the-wild/>
3. <http://blog.webroot.com/2013/04/02/spamvertised-re-changelog-as-promised-themed-emails-lead-to-malware/>
4. <http://blog.webroot.com/2013/04/03/cybercrime-friendly-service-offers-access-to-tens-of-thousands-of-compromised-accounts/>
5. <http://blog.webroot.com/2013/04/04/madimahdiflashback-os-x-connected-malware-spreading-through-skype/>
6. <http://blog.webroot.com/2013/04/05/cybercriminals-selling-valid-business-cards-data-of-company-executives-across-multiple-verticals/>
7. <http://blog.webroot.com/2013/04/08/a-peek-inside-the-zero-kit0kitring0-bundle-bootkit/>

8. <http://blog.webroot.com/2013/04/09/diy-skype-ring-flooder-offered-for-sale/>

9. <http://blog.webroot.com/2013/04/10/spamvertised-your-order-for-helicopter-for-the-weekend-themed-emails-lead-to-malware/>

10. <http://blog.webroot.com/2013/04/11/a-peek-inside-a-life-cycle-aware-underground-market-ad-for-a-private-keylogger/>

11. <http://blog.webroot.com/2013/04/12/american-airlines-you-can-download-your-ticket-themed-emails-lead-to-malware/>

12. <http://blog.webroot.com/2013/04/15/cybercriminals-offer-spam-friendly-smtp-servers-for-rent/>

13. <http://blog.webroot.com/2013/04/16/how-mobile-spammers-verify-the-validity-of-harvested-phone-numbers-part-two/>

14. <http://blog.webroot.com/2013/04/17/a-peek-inside-a-cracked-commercially-available-rat-remote-access-tool/>

15. <http://blog.webroot.com/2013/04/18/diy-russian-mobile-number-harvesting-tool-spotted-in-the-wild/>

16. <http://blog.webroot.com/2013/04/19/diy-sip-based-tdos-toolnumber-validity-checker-offered-for-sale/>
17. <http://blog.webroot.com/2013/04/23/captcha-solving-russian-email-account-registration-tool-helps-facilitate-cybercrime/>
18. <http://blog.webroot.com/2013/04/24/historical-osint-the-boston-marathon-explosion-and-fertilizer-plant-explosion-in-texas-themed-malware-campaigns/>
19. <http://blog.webroot.com/2013/04/25/fake-dhl-delivery-report-themed-emails-lead-to-malware/>
20. <http://blog.webroot.com/2013/04/26/cybercriminals-impersonate-bank-of-america-bofa-serve-malware/>
21. <http://blog.webroot.com/2013/04/29/how-fraudulent-blackhat-seo-monetizers-apply-quality-assurance-qa-to-their-diy-doorway-generators/>
22. <http://blog.webroot.com/2013/04/30/managed-russian-ransomware-as-a-service-spotted-in-the-wild/>
23. <http://ddanchev.blogspot.com/>
24. <http://twitter.com/danchodanchev>



Fake 'Facebook Profile Spy Application' Campaign Spreading Across Facebook (2013-05-24 18:58)

Over the last couple of days, multi-tasking cybercriminals have been spreading a "Facebook Profile Spy" campaign across Facebook, enticing users into installing a rogue Chrome extension, next to monetizing the campaign through

an unethical pseudo-mobile marketing agency, known as Prizerally.

Sample redirection chain:

hxxps://www.facebook.com/pages/Hajmc1rnjr/172683159561584?sk=app

_190322544333196

&9DyG45

->

hxxp://horribleapps.com

->

hxxp://terribleapps.com

->

hxxps://chrome.google.com/webstore/detai-

l/oacggeibdmjpmecojanlbbngabki

ncif

->

hxxp://www.picapplication.com/profile/last.html?1

->

hxxp://flightdealsrome.net/?subid=4563 ->

hxxp://lp.prizerally.com

148



Domain names reconnaissance:

horribleapps.com - 66.150.99.179 (**picovator.com**) -
Email: Masterjx12@gmail.com

terribleapps.com - 66.150.99.21 (**puzzledapps.com**;
testyapps.com) - Email: Masterjx12@gmail.com

picapplication.com - 66.150.99.179 - Email:
joshuarhodes1989@gmail.com

flightdealsrome.net - 174.140.17.100

prizerally.com - 46.19.35.207 - Email:
domains@mypengomobile.com

**We also got the following fraudulent and
typosquatted domains known to have responded to
the same IP**

(174.140.17.100) in the past:

0418490819.com

149

20.tv

2020testing.net

aaacomtests.net

aaacontests.net

aaamathtests.net

accordput.net

aceonlinetest.com

activetester.com

adjustfit.net

adjustpair.net

adjusttie.net

adslim.com

adventuretester.com

aidonlinesurveys.com

airplanetester.com

alignhang.net

alignmake.net

aliketester.com

allosurvey.net

amatuercumshots.org

analyzequiz.net

animalplanet.net

animereak.tv

answeringonlinesurveys.com

apptitudeonlinetest.com

arcosurvey.net

attuneeven.net

attunefix.net

attunehang.net

attunemake.net

attunepair.net

attunetune.net

avizoon.com

azdes.org

bajarvideo.com

balanceattune.net

balancecollate.net

balanceconnect.net

balancecounteract.net

balanceeven-steven.net

balancefocus.net

balancelevel.net

balanceneutralize.net

balancenullify.net

balanceoverhaul.net

balancerectify.net

balancesymmetry.net

balancetighten.net

bargainonlinetest.com

bensurvey.net

150

bestgetpaidonlinesurveys.com

bestonlinesurveysformoney.com

bestonlinesurveysforpay.com

bestonlinesurveyswebsite.com

bestprizedraw.com

bestratedonlinesurveys.com

bestwebquiz.net

bigpaidonlinesurveys.com

bitsonlinetest.com

blackgaygalleries.com

bletsurvey.net

blosurvey.net

bobmarly.com

bollywoodringtonessite.com

bret.com

bringgrind.net

bringtie.net

builbabear.com

buildonlinesurveys.com

cancelfix.net

cansafelist.com

carquestionswebsite.com

censurvey.net

challengequizonline.net

cheaponlinetests.com

chinabestlink.com

clickbusinessinfo.net

coinsurvey.net

collegeonlinetests.com

commercenetweb.com

compeitionstowinprizes.com

coolfreequizzes.com

cooponmom.net

countest.net

couponso.net

crazyonlinequizzes.com

creativelinkusa.com

cuteonlinequizzes.com

descargapeliculas.com

dfedex.com

didiwinaprize.net

discountonlinetests.com

dogquizzes.net

dotnetlink.com

downloadsmovies.com

easyonlinetesting.com

eicosurvey.net

employersonlinetest.com

englishonlinetest.com

etestonlinetesting.com

151

examxonlinetesting.com

exposurvey.net

farbestsurvey.net

fastrackonlinesurveys.com

fastsurveyworld.net

fbso.com

findonlinesurveysforcash.com

fletsurvey.net

fnnyvideo.com

fontest.net

free-live-xxx-cams.com

friendsonlinequiz.com

fuck-me-now.com

funonlinequizsurvey.com

funonlinequizteen.com

funonlinequizzesforkids.com

gay-sex-pics-porn-pictures-gay-sex-porn-gay-sex-pics-gay.com

generalonlinequiz.com

generatest.net

geocites.com

getpageranks.com

googledark.com

googlemx.com

googletraductor.com

googleunclesam.com

googllemaps.com

gooyoutube.com

granny.ca

gsd.com

gyoutube.com

hack-facebook.com

hkatb.adsldns.org

hohotmail.com

holder.me

holidaytravelpassport.net

hotmailm.com

hotmauil.com

hpforsale.org

internet-questions.net

ioutube.com

jkert.com

joinsurvey.net

kemert.com

kerosurvey.net

kogregate.com

kurosurvey.net

landminesurvey.net

latinswomen.com

letsurvey.net

lolita.org

152

loveonlinequiz.com

marilyn.com

medialinksite.com

mensurvey.net

mfacebook.com

miniclip.cl

minsurvey.net

mobiasbank.com

monicatubes.com

movietickits.com

msdip.com

mycosurvey.net

myford.com

notyoutube.com

ohotmail.com

oijwef.com

onlinemedsforall.net.in

onlinequize.com

outsurvey.net

pharmaonline.net.in

pina.com

pollings.net

pollinois.net

pollinoise.net

pollison.net

pollist.net

pollower.net

pollquestionsitewhhdh.com

pollustry.net

pollutan.net

poutsurvey.net

question-answer-website.com

questionansweringwebsites.com

questionanswerstudy.net

questionexams.net

questionforthequiz.com

questionnairesamplesurvey.com

questionpersonalityquiz.net

questionpollguide.net

questionquizsite.net

questionquizworld.net

questionsforasurvey.com

questionsitesell.com

questionssurveys.com

questionsurveyfriend.com

quicksurveydirect.net

quizbull.net

quizbulla.net

quizbullah.net

quizbullen.net

153

quizbulles.net

quizbust.net

quizbustav.net

quizbustin.net

quizbustle.net

quizbustom.net

quizbustry.net

quizin.net

quizingles.net

quizingly.net

quizquestionsite.net

quizzeri.net

quizzerial.net

quizzeris.net

quizzerish.net

redirectofferpage.com

reinsurvey.net

rentube.com

rep.ppmate.com

repeatest.net

ruralaresdubai.net.in

sappygirls.com

scensurvey.net

securitytube.com

seehomevids.com

stratest.net

sumotorrents.com

sunsurvey.net

superquestionquiz.net

supersurveygroup.net

supersurveysite.net

survey-masters.net

2surveyablsoute.net

surveyaboutyou.net

surveyacout.net

surveyalot.net

surveyanyone.net

surveyask.net

surveyassistant.net

surveylatest.net

surveyorster.net

susan.com

testabled.net

testables.net

testabling.net

testand.net

testants.net

testatus.net

testaura.net

testaustralia.com

154

testeradjective.com

testeradvice.com

testeraid.com

testic.net

testical.net

testige.net

testigious.net

testingacademy.net

testingadvantage.net

testingadvice.net

testingadwords.net

testingagainagain.net

testingame.net

testion.net

testivate.net

testself.net

tetsurvey.net

thegreatanswer.com

thenamequiz.net

thequestionpoll.net

thesurveyresearch.net

thosurvey.net

tmobilw.com

toutsurvey.net

toyotest.net

tsurvey.net

tube99.com

tunehang.net

tunelevel.net

tunemake.net

tuneoppose.net

tuneparity.net

tuneservice.net

tuneset.net

tunesteady.net

tunetie.net

twittee.com

unionbank.org

unsurvey.net

update.ppmate.com

usagreatlink.com

vacationcellular.net

vintagetownbazar.co.in

watchyoutube.com

webwordquiz.net

weighfit.net

weighmake.net

weighmend.net

weighparity.net

weighpolish.net

155

weightighten.net

wesurvey.net

wickapidea.com

wickepidia.com

worldcityonline.com

wuizforcash.com

www-yuotube.com

www.ammoneta.com

www.downloadsmovies.com

www.foxchannel.com

www.hack-facebook.com

www.securitytube.com

www.tmobilw.com

www.windycitywatchdog.com

www.youtrube.com

www.youtubemobile.com

www.youtuve.com

wwwquestionnairesurveys.com

wwwtoutube.com

yahoomailk.com

yaotube.com

yautube.com

yootube.com

yotobe.com

youbube.com

yourhomesurvey.net

yourownsurvey.net

yoursurveysite.net

yourtopsite.com

youtsurvey.net

youtubemobile.com

youtubi.com

youtuhe.com

youtuve.com

ypoutube.com

yuvuty.com

zerosurvey.net

156



As well as the following malicious MD5s phoning back to the same IP in the past:

[1]MD5: e315a877c58773ce82cc32fc192bdfa5

[2]MD5: 1cd4c2a2b2143689b185e064dc6c331c

[3]MD5: 26c5102e75daf3d3c696ad719bc55ad4

Prizerally's scheme is fairly simple:

Service costs £3 per question played and a £4,50 sign up fee applies. You will receive an additional £1.50 charge

157

for a reminder message tomorrow. Winners will be contacted every first businessweek of the month, all question entries must be received before 00.00 on the last day of the month. This is not a subscription service. Minimum age

18+ with bill payer's permission. One prize available per service per month. Customer service: call 0800 408 0796,

*email uk@prizerally.com or visit the website:
www.prizerally.com. Play the game on your mobile. The
winner will be*

*selected among all participants in the first business week of
every month. When participating you acknowledge that*

*you agree to the terms & conditions, you are a resident of
the UK, 18 years or older and authorized account holder
and/or that you have the consent of the accountholder. £3
per question. This service is a product of Mypengo Mobile.*

*Free entry method: send an email with your name,
phonenumber, and prize you want to win to
info@prizerally.com.*

*Prizerally is not affiliated with, sponsored by or endorsed by
any of the listed products or retailers. Trademarks,*

*service marks, logos (including, without limitation, the
individual names of products and retailers) are the property*

*of their respective owners. When you see one of our
Products on the Internet, you can start receiving our content*

*via SMS (i.e. text message). You can enter your mobile
telephone number on the landing pages via the Internet*

*and confirm your registration. You hereby agree to the
Terms and Conditions. Prizerally charges you £3,00 per*

*question played. Each sent answer will be followed by a new
question. If you stop sending answers you will not*

*receive any more messages. Once stopped you will receive
one extra £1,50 reminder message. To stop this message,*

simply text STOP to 85150. From this moment on you have to decide on your own if you will continue to play for

more points. By answering a question, you will receive a new messages containing a new puzzel/question also

chargeble at £ 1,50 per text message received. When you stop sending answers the game will end. O2 and Orange

customers can only spend the maximum amount of £ 30.00 a day. This spending cap applies for one day, so the next

day these customers are eligible to play again. The maximum amount you can spend on our Prizerally service is £ 99.00.

Facebook has been notified. The rogue Chrome extension has already been removed.

This post has been reproduced from [4]Dancho Danchev's blog. Follow him [5]on Twitter.

1.

<https://www.virustotal.com/en/file/0329bd90de1ad1608bfe91210b66929caeb99a0574bb1008123b95c7b1b0e756/analysis/>

[is/](#)

2.

<https://www.virustotal.com/en/file/35c970ae66dde7688e55a87860c8bc60d8ab3f502437448e0ea60dfc19659499/analysis/>

[is/](#)

3.

<https://www.virustotal.com/en/file/58337863b283dfcc03fef8614a821b2b63fb018cb14f2353e97da4d42110b6d1/analysis/>

[is/](#)

4. <http://ddanchev.blogspot.com/>

5. <http://twitter.com/danchodanchev>

158



Fake 'Facebook Profile Spy Application' Campaign Spreading Across Facebook (2013-05-24 18:58)

Over the last couple of days, multi-tasking cybercriminals have been spreading a "Facebook Profile Spy" campaign across Facebook, enticing users into installing a rogue Chrome extension, next to monetizing the campaign through

an unethical pseudo-mobile marketing agency, known as Prizerally.

Sample redirection chain:

hxxps://www.facebook.com/pages/Hajmc1rnjr/172683159561584?sk=app

_190322544333196

&9DyG45

->

hxxp://horribleapps.com

->

hxxp://terribleapps.com

->

hxxps://chrome.google.com/webstore/detai-

l/oacggeibdmjpmecojanlbbngabki

ncif

->

hxxp://www.picapplication.com/profile/last.html?1

->

hxxp://flightdealsrome.net/?subid=4563 ->

hxxp://lp.prizerally.com

159



Domain names reconnaissance:

horribleapps.com - 66.150.99.179 (**picovator.com**) -
Email: Masterjx12@gmail.com

terribleapps.com - 66.150.99.21 (**puzzledapps.com;**
testyapps.com) - Email: Masterjx12@gmail.com

picapplication.com - 66.150.99.179 - Email:
joshuarhodes1989@gmail.com

flightdealsrome.net - 174.140.17.100

prizerally.com - 46.19.35.207 - Email:
domains@mypengomobile.com

**We also got the following fraudulent and
typosquatted domains known to have responded to
the same IP**

(174.140.17.100) in the past:

0418490819.com

160

20.tv

2020testing.net

aaacomtests.net

aaacontests.net

aaamathtests.net

accordput.net

aceonlinetest.com

activetester.com

adjustfit.net

adjustpair.net

adjusttie.net

adslim.com

adventuretester.com

aidonlinesurveys.com

airplanetester.com

alignhang.net

alignmake.net

aliketester.com

allosurvey.net

amatuercumshots.org

analyzequiz.net

animalplanet.net

animereak.tv

answeringonlinesurveys.com

apptitudeonlinetest.com

arcosurvey.net

attuneeven.net

attunefix.net

attunehang.net

attunemake.net

attunepair.net

attunetune.net

avizoon.com

azdes.org

bajarvideo.com

balanceattune.net

balancecollate.net

balanceconnect.net

balancecounteract.net

balanceeven-steven.net

balancefocus.net

balancelevel.net

balanceneutralize.net

balancenullify.net

balanceoverhaul.net

balancerectify.net

balancesymmetry.net

balancetighten.net

bargainonlinetest.com

bensurvey.net

161

bestgetpaidonlinesurveys.com

bestonlinesurveysformoney.com

bestonlinesurveysforpay.com

bestonlinesurveyswebsite.com

bestprizedraw.com

bestratedonlinesurveys.com

bestwebquiz.net

bigpaidonlinesurveys.com

bitsonlinetest.com

blackgaygalleries.com

bletsurvey.net

blosurvey.net

bobmarly.com

bollywoodringtonessite.com

bret.com

bringgrind.net

bringtie.net

builbabear.com

buildonlinesurveys.com

cancelfix.net

cansafelist.com

carquestionswebsite.com

censurvey.net

challengequizonline.net

cheaponlinetests.com

chinabestlink.com

clickbusinessinfo.net

coinsurvey.net

collegeonlinetests.com

commercenetweb.com

compeitionstowinprizes.com

coolfreequizzes.com

cooponmom.net

countest.net

couponso.net

crazyonlinequizzes.com

creativelinkusa.com

cuteonlinequizzes.com

descargapeliculas.com

dfedex.com

didiwinaprize.net

discountonlinetests.com

dogquizzes.net

dotnetlink.com

downloadsmovies.com

easyonlinetesting.com

eicosurvey.net

employersonlinetest.com

englishonlinetest.com

etestonlinetesting.com

162

examxonlinetesting.com

exposurvey.net

farbestsurvey.net

fastrackonlinesurveys.com

fastsurveyworld.net

fbso.com

findonlinesurveysforcash.com

fletsurvey.net

fnnyvideo.com

fontest.net

free-live-xxx-cams.com

friendsonlinequiz.com

fuck-me-now.com

funonlinequizsurvey.com

funonlinequizteen.com

funonlinequizzesforkids.com

gay-sex-pics-porn-pictures-gay-sex-porn-gay-sex-pics-gay.com

generalonlinequiz.com

generatest.net

geocites.com

getpageranks.com

googledark.com

googlemx.com

googletraductor.com

googleunclesam.com

googllemaps.com

gooyoutube.com

granny.ca

gsd.com

gyoutube.com

hack-facebook.com

hkatb.adsldns.org

hohotmail.com

holder.me

holidaytravelpassport.net

hotmailm.com

hotmauil.com

hpforsale.org

internet-questions.net

ioutube.com

jkert.com

joinsurvey.net

kemert.com

kerosurvey.net

kogregate.com

kurosurvey.net

landminesurvey.net

latinswomen.com

letsurvey.net

lolita.org

163

loveonlinequiz.com

marilyn.com

medialinksite.com

mensurvey.net

mfacebook.com

miniclip.cl

minsurvey.net

mobiasbank.com

monicatubes.com

movietickits.com

msdip.com

mycosurvey.net

myford.com

notyoutube.com

ohotmail.com

oijwef.com

onlinemedsforall.net.in

onlinequize.com

outsurvey.net

pharmaonline.net.in

pina.com

pollings.net

pollinois.net

pollinoise.net

pollison.net

pollist.net

pollower.net

pollquestionsitewhdh.com

pollustry.net

pollutan.net

poutsurvey.net

question-answer-website.com

questionansweringwebsites.com

questionanswerstudy.net

questionexams.net

questionforthequiz.com

questionnairesamplesurvey.com

questionpersonalityquiz.net

questionpollguide.net

questionquizsite.net

questionquizworld.net

questionsforasurvey.com

questionsitesell.com

questionssurveys.com

questionsurveyfriend.com

quicksurveydirect.net

quizbull.net

quizbulla.net

quizbullah.net

quizbullen.net

164

quizbulles.net

quizbust.net

quizbustav.net

quizbustin.net

quizbustle.net

quizbustom.net

quizbustry.net

quizin.net

quizingles.net

quizingly.net

quizquestionsite.net

quizzeri.net

quizzerial.net

quizzeris.net

quizzerish.net

redirectofferpage.com

reinsurvey.net

rentube.com

rep.ppmate.com

repeatest.net

ruralaresdubai.net.in

sappygirls.com

scensurvey.net

securitytube.com

seehomevids.com

stratest.net

sumotorrents.com

sunsurvey.net

superquestionquiz.net

supersurveygroup.net

supersurveysite.net

survey-masters.net

2surveyablsoute.net

surveyaboutyou.net

surveyacout.net

surveyalot.net

surveyanyone.net

surveyask.net

surveyassistant.net

surveylatest.net

surveyorster.net

susan.com

testabled.net

testables.net

testabling.net

testand.net

testants.net

testatus.net

testaura.net

testaustralia.com

165

testeradjective.com

testeradvice.com

testeraid.com

testic.net

testical.net

testige.net

testigious.net

testingacademy.net

testingadvantage.net

testingadvice.net

testingadwords.net

testingagainagain.net

testingame.net

testion.net

testivate.net

testself.net

tetsurvey.net

thegreatanswer.com

thenamequiz.net

thequestionpoll.net

thesurveyresearch.net

thosurvey.net

tmobilw.com

toutsurvey.net

toyotest.net

tsurvey.net

tube99.com

tunehang.net

tunelevel.net

tunemake.net

tuneoppose.net

tuneparity.net

tuneservice.net

tuneset.net

tunesteady.net

tunetie.net

twittee.com

unionbank.org

unsurvey.net

update.ppmate.com

usagreatlink.com

vacationcellular.net

vintagetownbazar.co.in

watchyoutube.com

webwordquiz.net

weighfit.net

weighmake.net

weighmend.net

weighparity.net

weighpolish.net

166

weightighten.net

wesurvey.net

wickapidea.com

wickepidia.com

worldcityonline.com

wuizforcash.com

www-yuotube.com

www.ammoneta.com

www.downloadsmovies.com

www.foxchannel.com

www.hack-facebook.com

www.securitytube.com

www.tmobilw.com

www.windycitywatchdog.com

www.yotrube.com

www.youtubemobile.com

www.youtuve.com

wwwquestionnairesurveys.com

wwwtoutube.com

yahoomailk.com

yaotube.com

yautube.com

yootube.com

yotobe.com

youbube.com

yourhomesurvey.net

yourownsurvey.net

yoursurveysite.net

yourtopsite.com

youtsurvey.net

youtubemobile.com

youtubi.com

youtuhe.com

youtuve.com

ypoutube.com

yuvuty.com

zerosurvey.net

167



As well as the following malicious MD5s phoning back to the same IP in the past:

[1]MD5: e315a877c58773ce82cc32fc192bdfa5

[2]MD5: 1cd4c2a2b2143689b185e064dc6c331c

[3]MD5: 26c5102e75daf3d3c696ad719bc55ad4

Prizerally's scheme is fairly simple:

Service costs £3 per question played and a £4,50 sign up fee applies. You will receive an additional £1.50 charge

168

*for a reminder message tomorrow. Winners will be contacted every first businessweek of the month, all question entries must be received before 00.00 on the last day of the month. This is not a subscription service.
Minimum age*

18+ with bill payer's permission. One prize available per service per month. Customer service: call 0800 408 0796,

*email uk@prizerally.com or visit the website:
www.prizerally.com. Play the game on your mobile. The winner will be*

selected among all participants in the first business week of every month. When participating you acknowledge that

you agree to the terms & conditions, you are a resident of the UK, 18 years or older and authorized account holder and/or that you have the consent of the accountholder. £3 per question. This service is a product of Mypengo Mobile.

Free entry method: send an email with your name, phonenumber, and prize you want to win to info@prizerally.com.

Prizerally is not affiliated with, sponsored by or endorsed by any of the listed products or retailers. Trademarks,

service marks, logos (including, without limitation, the individual names of products and retailers) are the property

of their respective owners. When you see one of our Products on the Internet, you can start receiving our content

via SMS (i.e. text message). You can enter your mobile telephone number on the landing pages via the Internet

and confirm your registration. You hereby agree to the Terms and Conditions. Prizerally charges you £3,00 per

question played. Each sent answer will be followed by a new question. If you stop sending answers you will not

receive any more messages. Once stopped you will receive one extra £1,50 reminder message. To stop this message,

simply text STOP to 85150. From this moment on you have to decide on your own if you will continue to play for

more points. By answering a question, you will receive a new messages containing a new puzzel/question also

chargeble at £ 1,50 per text message received. When you stop sending answers the game will end. O2 and Orange

customers can only spend the maximum amount of £ 30.00 a day. This spending cap applies for one day, so the next

day these customers are eligible to play again. The maximum amount you can spend on our Prizerally service is £ 99.00.

Facebook has been notified. The rogue Chrome extension has already been removed.

Updates will be posted as soon as new developments take place.

1.

<https://www.virustotal.com/en/file/0329bd90de1ad1608bfe91210b66929caeb99a0574bb1008123b95c7b1b0e756/analysis/>

[is/](#)

2.

<https://www.virustotal.com/en/file/35c970ae66dde7688e55a87860c8bc60d8ab3f502437448e0ea60dfc19659499/analysis/>

[is/](#)

3.

<https://www.virustotal.com/en/file/58337863b283dfcc03fef8614a821b2b63fb018cb14f2353e97da4d42110b6d1/analysis/>

[is/](#)

169



A Peek Inside the Russian Underground Market for Fake Documents/IDs/Passports (2013-05-25 18:52)

[1]**Fake IDs/fake passports** have always been a hot
[2]**commodity within the cybercrime ecosystem.**

Thanks to their general availability and affordable prices – naturally based on the quality that a potential cybercriminal/fraudster is seeking – the vendors behind them continue undermining the trust chain that society/market thrives

on, by empowering cybercriminals and fugitives with new IDs to be later on used in related fraudulent activities.

In this post, I'll sample fraudulent activity on the Russian underground marketplace, feature exclusive screen-

shots of fake passports currently offered for sale, and discuss how relatively low profile cybercriminals have been

literally generating fake (Russian) passports for years, primarily relying on DIY passport/stamp generating tools.

Sample screenshots of the inventory of available fake passports for multiple countries:

170



171



172



173



174



175



176



177



178



179



180



181



182



183



184



185



186



187



188



189



190



191



192



193



194



Affected countries include: Russia, Belarus, Canada, Germany, Denmark, Finland, Israel, Netherlands (Holland),

Norway, Romania, United Kingdom, United States, Australia, Ukraine. The prices vary between \$20-30, and according

to the vendors, use real people's data/photos etc.

It's also worth emphasizing on the fact that, of all the countries, Russia's underground marketplace for fake

documents is perhaps the most vibrant one. Next to high-quality fake documents/IDs/passports, they're naturally

the cheap alternatives, which Russian fraudsters have been literally generating for years, relying on DIY (do-it-yourself) tools/stamp editors like these:

195



196



197



Thanks to the demand for such kind of underground market assets, I'm certain that that market would continue

flourishing, and would eventually reach a stage where the vendors would start sacrificing OPSEC (Operational

Security) in an attempt to reach customers from virtually every country. With localization on demand services

proliferating, next to the ubiquitous for the cybercrime ecosystem, affiliate based revenue-sharing models, vendors

of fake documents/IDs/passports, have virtually everything that they need at their disposal, if they were to start

targeting the international audience.

This post has been reproduced from [3]Dancho Danchev's blog. Follow him [4]on Twitter.

1. http://www.team-cymru.com/ReadingRoom/Whitepapers/2010/FakeID_in_the_Underground_Economy.pdf
2. <http://ddanchev.blogspot.com/2011/10/exposing-market-for-stolen-credit-cards.html>
3. <http://ddanchev.blogspot.com/>
4. <http://twitter.com/danchodanchev>

198



A Peek Inside the Russian Underground Market for Fake Documents/IDs/Passports (2013-05-25 18:52)

[1]**Fake IDs/fake passports** have always been a hot
[2]**commodity within the cybercrime ecosystem.**

Thanks to their general availability and affordable prices – naturally based on the quality that a potential cybercriminal/fraudster is seeking – the vendors behind them continue undermining the trust chain that society/market thrives on, by empowering cybercriminals and fugitives with new IDs to be later on used in related fraudulent activities.

In this post, I'll sample fraudulent activity on the Russian underground marketplace, feature exclusive screenshots of fake passports currently offered for sale, and discuss how relatively low profile cybercriminals have been literally generating fake (Russian) passports for years, primarily relying on DIY passport/stamp generating tools.

Sample screenshots of the inventory of available fake passports for multiple countries:

199



200



201



202





203



204



205



206



207



208



209



210



211



212



213



214



215



216



217



218



219



220



221



222



223



Affected countries include: Russia, Belarus, Canada, Germany, Denmark, Finland, Israel, Netherlands (Holland),

Norway, Romania, United Kingdom, United States, Australia, Ukraine. The prices vary between \$20-30, and according

to the vendors, use real people's data/photos etc.

It's also worth emphasizing on the fact that, of all the countries, Russia's underground marketplace for fake

documents is perhaps the most vibrant one. Next to high-quality fake documents/IDs/passports, they're naturally

the cheap alternatives, which Russian fraudsters have been literally generating for years, relying on DIY (do-it-yourself) tools/stamp editors like these:

224



225



226



Thanks to the demand for such kind of underground market assets, I'm certain that that market would continue flour-

ishing, and would eventually reach a stage where the vendors would start sacrificing OPSEC (Operational Security)

in an attempt to reach customers from virtually every country. With localization on demand services proliferating, next to the ubiquitous for the cybercrime ecosystem, affiliate based revenue-sharing models, vendors of fake documents/IDs/passports, have virtually everything that they need at their disposal, if they were to start targeting the international audience.

1. http://www.team-cymru.com/ReadingRoom/Whitepapers/2010/FakeID_in_the_Underground_Economy.pdf
2. <http://ddanchev.blogspot.com/2011/10/exposing-market-for-stolen-credit-cards.html>

227

1.6

June

228



Summarizing Webroot's Threat Blog Posts for May (2013-06-04 15:24)

The following is a brief summary of all of my posts at [1]**Webroot's Threat Blog** for May, 2013. You can subscribe to

[2]**Webroot's Threat Blog RSS Feed**, or follow me on Twitter:

- 01.** [3]FedWire 'Your Wire Transfer' themed emails lead to malware
- 02.** [4]A peek inside a CVE-2013-0422 exploiting DIY malicious Java applet generating tool
- 03.** [5]New IRC/HTTP based DDoS bot wipes out competing malware
- 04.** [6]New version of DIY Google Dorks based mass website hacking tool spotted in the wild
- 05.** [7]Citibank 'Merchant Billing Statement' themed emails lead to malware
- 06.** [8]Fake Amazon 'Your Kindle E-Book Order' themed emails circulating in the wild, lead to client-side exploits and malware
- 07.** [9]Cybercriminals impersonate New York State's Department of Motor Vehicles (DMV), serve malware
- 08.** [10]Cybercriminals offer HTTP-based keylogger for sale, accept Bitcoin
- 09.** [11]Newly launched E-shop for hacked PCs charges based on malware 'executions'
- 10.** [12]New subscription-based 'stealth Bitcoin miner' spotted in the wild
- 11.** [13]Fake 'Free Media Player' distributed via rogue 'Adobe Flash Player HD' advertisement

229

- 12.** [14]Newly launched 'Magic Malware' spam campaign relies on bogus 'New MMS' messages

- 13.** [15]Commercial 'form grabbing' rootkit spotted in the wild
- 14.** [16]DIY malware cryptor as a Web service spotted in the wild – part two
- 15.** [17]CVs and sensitive info soliciting email campaign impersonates NATO
- 16.** [18]New commercially available DIY invisible Bitcoin miner spotted in the wild
- 17.** [19]Fake 'Export License/Payment Invoice' themed emails lead to malware
- 18.** [20]Compromised Indian government Web site leads to Black Hole Exploit Kit
- 19.** [21]Cybercriminals resume spamvertising Citibank 'Merchant Billing Statement' themed emails, serve malware
- 20.** [22]Marijuana-themed DDoS for hire service spotted in the wild
- 21.** [23]Fake 'Vodafone U.K Images' themed malware serving spam campaign circulating in the wild

This post has been reproduced from [24]Dancho Danchev's blog. Follow him [25]on Twitter.

- 1. <http://blog.webroot.com/>
- 2. <http://feeds2.feedburner.com/WebrootThreatBlog>
- 3. <http://blog.webroot.com/2013/05/01/fedwire-your-wire-transfer-themed-emails-lead-to-malware/>

4. <http://blog.webroot.com/2013/05/02/a-peek-inside-a-cve-2013-0422-exploiting-diy-malicious-java-applet-generating-tool/>

5. <http://blog.webroot.com/2013/05/03/new-irchttp-based-ddos-bot-wipes-out-competing-malware/>

6. <http://blog.webroot.com/2013/05/06/new-version-of-diy-google-dorks-based-mass-website-hacking-tool-spotted-in-the-wild/>

7. <http://blog.webroot.com/2013/05/07/citibank-merchant-billing-statement-themed-emails-lead-to-malware/>

8. <http://blog.webroot.com/2013/05/08/fake-amazon-your-kindle-e-book-order-themed-emails-circulating-in-the-wild-lead-to-client-side-exploits-and-malware/>

9. <http://blog.webroot.com/2013/05/09/cybercriminals-impersonate-new-york-states-department-of-motor-vehicles-dmv-serve-malware/>

10. <http://blog.webroot.com/2013/05/10/cybercriminals-offer-http-based-keylogger-for-sale-accept-bitcoin/>

11.

<http://blog.webroot.com/2013/05/13/newly-launched-e-shop-for-hacked-pcs-charges-based-on-malware-executions/>

12. <http://blog.webroot.com/2013/05/14/new-subscription-based-stealth-bitcoin-miner-spotted-in-the-wild/>

13.

<http://blog.webroot.com/2013/05/15/fake-free-media-player-distributed-via-rogue-adobe-flash-player-hd-advertisement/>

14.

<http://blog.webroot.com/2013/05/17/newly-launched-magic-malware-spam-campaign-relies-on-bogus-new-mms-messages/>

15. <http://blog.webroot.com/2013/05/17/commercial-form-grabbing-rootkit-spotted-in-the-wild/>

16. <http://blog.webroot.com/2013/05/20/diy-malware-cryptor-as-a-web-service-spotted-in-the-wild-part-two/>

17. <http://blog.webroot.com/2013/05/21/cvs-and-sensitive-info-soliciting-email-campaign-impersonates-nato/>

18. <http://blog.webroot.com/2013/05/22/new-commercially-available-diy-invisible-bitcoin-miner-spotted-in-the-wild/>

19. <http://blog.webroot.com/2013/05/23/fake-export-licensepayment-invoice-themed-emails-lead-to-malware/>

20.

<http://blog.webroot.com/2013/05/24/compromised-indian-government-web-site-leads-to-black-hole-exploit-kit/>

21. <http://blog.webroot.com/2013/05/29/cybercriminals-resume-spamvertising-citibank-merchant-billing-statement-themed-emails-serve-malware/>

22. <http://blog.webroot.com/2013/05/30/marijuana-themed-ddos-for-hire-service-spotted-in-the-wild/>

23.

<http://blog.webroot.com/2013/05/31/fake-vodafone-uk-images-themed-malware-serving-spam-campaign-circulating-in-the-wild/>

24. <http://ddanchev.blogspot.com/>

25. <http://twitter.com/danchodanchev>

230



Malware-Serving "Who's Viewed Your Facebook Profile" Campaign Spreading Across Facebook

(2013-06-10 15:07)

A currently ongoing Facebook spreading malware-serving campaign, entices users into downloading and executing

a malicious executable, pretending to be a " *Who's Viewed Your Facebook Profile*" extension. In reality though, the executable, part of a campaign that's been ongoing for several months, will steal private information from local

browsers, will auto-start on Windows startup, and will attempt to infect all of the victim's friends across Facebook.

The executable, including several other related executables part of the campaign, are currently hosted on Google

Code, and according to Google Code's statistics, one of the malicious files has already been downloaded 1,870,788

times. Surprisingly, the Coode Project is called " *Project Don't Download*". Very interesting self-contradicting social engineering attempt.

Let's dissect the campaign, list the domain's portfolio used in it, provide detection rates for the malicious exe-

cutables, and connect the campaign to multiple other campaigns observed in the wild over the last couple of weeks.

[1]

231



Sample redirection chain:

hxxp://cnlz3.tk/?2959858

->

hxxp://profilelo.8c1.net/

->

hxxp://profileste.uni.me/?skuwjjsadsuquwhdas

->

*hxxps://project-dont-download.googlecode.com/files/Profile
%20View %20- %205v2.exe*

Subdomain reconnaissance:

profilelo.8c1.net - 82.208.40.3

profileste.uni.me - 198.23.52.98

project-dont-download.googlecode.com - Email:
mergimi14@live.com

Detection rate for the malicious executable: [2]**MD5:**
c5b2247a37a8d26063af55c6c975782d - detected by
23

out of 47 antivirus scanners as JS:Clicker-P [Trj];
RDN/Generic.dx!chs

Once executed, the sample drops the following MD5s on the affected hosts:

MD5: 3729796a618de670128e80bb750dba35

MD5: bc5ea93000fd79cf3d874567068adfc5

MD5: 3448d5a74e86fdc88569df99dbc19c55

MD5: c3c67c3df487390dfdfa4890832b8a46

MD5: 161fff31429f1fcd99a56208cf9d2b58

MD5: c8dfbeb2e89a9557523b5a57619a9c44

MD5: b83d2283066c68e8cc448c578dd121aa

232



MD5: 0e254726843ed308ca142333ea0c5d28

MD5: cbb6e03d0b08ba4a8eeac1467921b7dd

MD5: a3ef72a0345a564bde3df2654f384a21

MD5: 123c9d897b74548aa6ce65b456a8b732

MD5: 181f01156f23d4e732a414eaa2f6b870

MD5: 74d4b4298bc6fe8871ad1aa654d347c6

Download statistics for the malicious executables hosted on Google Code:

Profile Viewer - 5.exe - 1,870,788 downloads

Profile Stalker - V.exe - 45983 downloads

Profile View - 5v2.exe - 9496 downloads

Profile Stalker - D.exe - 2 downloads

Detection rates for the malicious executables hosted on Google Code:

Profile Stalker - D.exe - [3]**MD5:**

c9220176786fe074de210529570959c5 - detected by 3 out of 47 antivirus scanners

as Trojan.AVKill.30538; JS/TrojanClicker.Agent.NDL

Profile Stalker - V.exe - [4]**MD5:**

a6073378d764e3af4cb289cac91b3f97 - detected by 24 out of 47 antivirus scanners

as JS/TrojanClicker.Agent.NDL; Trojan.Win32.Clicker!BT

Profile Viewer - 5.exe - [5]**MD5:**
814837294bc34f288e31637bab955e6c - detected by
24 out of 47 antivirus scanners

as Troj/Agent-ABOE

Samples phone back to the followind URLs/domains:

hxxp://stats.app-data.net/installer.gif?action=started

&browser=ie6

&ver=1

_26

_153

&bic=00A473047B09414785A7A54908970321E

&app=30413 &appver=0

&verifier=d3459d462f931be10f76456d86fe24d-5 &srcid=0

&subid=0 &zdata=0 &ff=0 &ch=0 &default=ie &os=XP32

&admin=1 &type=1 &asw=0

stats.app-data.net - 207.171.163.139

app-static.crossrider.com - 69.16.175.10

errors.app-data.net - 207.171.163.139

Facebook and Google have been notified.

This post has been reproduced from [6]Dancho Danchev's blog. Follow him [7]on Twitter.

1.

http://1.bp.blogspot.com/-lxZJezC4rz0/UbW86IHzcBI/AAAAAAAAAFu0/dmQ14sZpxgg/s1600/Whos_Viewed_Your_Facebook

[_Profile_Fake_Rogue_Extension.png](#)

2.

<https://www.virustotal.com/en/file/7b5f495dbc987f16c1f331141dd9dd62a8066503226d5bf457cbd5875515a600/analysis>

[233](#)

[is/](#)

3.

<https://www.virustotal.com/en/file/5a2729550420e40836fd2f5e2bb42fe4b9d36dd3fbb0f12fc05b829b5e295f80/analysis>

[is/1370862388/](#)

4.

<https://www.virustotal.com/en/file/07ac717f288cdee6c5b6ef4eeda86f90892ef26fd11c7aac11ea6401a7dcc2e6/analysis>

[is/1370862459/](#)

5.

<https://www.virustotal.com/en/file/de7e13991bbbe84c6470c070d675ceff1f07b3ff3c545ca53b33ebbc1790b9c9/analysis>

[is/1370862551/](#)

6. <http://ddanchev.blogspot.com/>

7. <http://twitter.com/danchodanchev>

234



Malware-Serving "Who's Viewed Your Facebook Profile" Campaign Spreading Across Facebook

(2013-06-10 15:07)

A currently ongoing Facebook spreading malware-serving campaign, entices users into downloading and executing

a malicious executable, pretending to be a " *Who's Viewed Your Facebook Profile*" extension. In reality though, the executable, part of a campaign that's been ongoing for several months, will steal private information from local

browsers, will auto-start on Windows startup, and will attempt to infect all of the victim's friends across Facebook.

The executable, including several other related executables part of the campaign, are currently hosted on Google

Code, and according to Google Code's statistics, one of the malicious files has already been downloaded 1,870,788

times. Surprisingly, the Code Project is called " *Project Don't Download*". Very interesting self-contradicting social engineering attempt.

Let's dissect the campaign, list the domain's portfolio used in it, provide detection rates for the malicious exe-

cutables, and connect the campaign to multiple other campaigns observed in the wild over the last couple of weeks.

[1]



Sample redirection chain:

hxxp://cnlz3.tk/?2959858

->

hxxp://profilelo.8c1.net/

->

hxxp://profileste.uni.me/?skuwjjsadsuquwhdas

->

*hxxps://project-dont-download.googlecode.com/files/Profile
%20View %20- %205v2.exe*

Subdomain reconnaissance:

profilelo.8c1.net - 82.208.40.3

profileste.uni.me - 198.23.52.98

project-dont-download.googlecode.com - Email:
mergimi14@live.com

Detection rate for the malicious executable: [2]**MD5:
c5b2247a37a8d26063af55c6c975782d** - detected by
23

out of 47 antivirus scanners as JS:Clicker-P [Trj];
RDN/Generic.dx!chs

Once executed, the sample drops the following MD5s on the affected hosts:

MD5: 3729796a618de670128e80bb750dba35

MD5: bc5ea93000fd79cf3d874567068adfc5

MD5: 3448d5a74e86fdc88569df99dbc19c55

MD5: c3c67c3df487390dfdfa4890832b8a46

MD5: 161fff31429f1fcd99a56208cf9d2b58

MD5: c8dfbeeb2e89a9557523b5a57619a9c44

MD5: b83d2283066c68e8cc448c578dd121aa

236



MD5: 0e254726843ed308ca142333ea0c5d28

MD5: cbb6e03d0b08ba4a8eeac1467921b7dd

MD5: a3ef72a0345a564bde3df2654f384a21

MD5: 123c9d897b74548aa6ce65b456a8b732

MD5: 181f01156f23d4e732a414eaa2f6b870

MD5: 74d4b4298bc6fe8871ad1aa654d347c6

**Download statistics for the malicious executables
hosted on Google Code:**

Profile Viewer - 5.exe - 1,870,788 downloads

Profile Stalker - V.exe - 45983 downloads

Profile View - 5v2.exe - 9496 downloads

Profile Stalker - D.exe - 2 downloads

Detection rates for the malicious executables hosted on Google Code:

Profile Stalker - D.exe - [3]**MD5:**

c9220176786fe074de210529570959c5 - detected by 3 out of 47 antivirus scanners

as Trojan.AVKill.30538; JS/TrojanClicker.Agent.NDL

Profile Stalker - V.exe - [4]**MD5:**

a6073378d764e3af4cb289cac91b3f97 - detected by 24 out of 47 antivirus scanners

as JS/TrojanClicker.Agent.NDL; Trojan.Win32.Clicker!BT

Profile Viewer - 5.exe - [5]**MD5:**

814837294bc34f288e31637bab955e6c - detected by 24 out of 47 antivirus scanners

as Troj/Agent-ABOE

Samples phone back to the followind URLs/domains:

hxxp://stats.app-data.net/installer.gif?action=started

&browser=ie6

&ver=1

_26

_153

&bic=00A473047B09414785A7A54908970321IE

&app=30413 &appver=0

&verifier=d3459d462f931be10f76456d86fe24d-5 &srcid=0

&subid=0 &zdata=0 &ff=0 &ch=0 &default=ie &os=XP32

&admin=1 &type=1 &asw=0

stats.app-data.net - 207.171.163.139

app-static.crossrider.com - 69.16.175.10

errors.app-data.net - 207.171.163.139

Facebook and Google have been notified.

Updates will be posted as soon as new developments take place.

1.

[http://1.bp.blogspot.com/-
lxZJezC4rz0/UbW86IHzcBI/AAAAAAAAAFu0/dmQ14sZpxgg/s
1600/Whos_Viewed_Your_Facebook
_Profile_Fake_Rogue_Extension.png](http://1.bp.blogspot.com/-lxZJezC4rz0/UbW86IHzcBI/AAAAAAAAAFu0/dmQ14sZpxgg/s1600/Whos_Viewed_Your_Facebook_Profile_Fake_Rogue_Extension.png)

2.

[https://www.virustotal.com/en/file/7b5f495dbc987f16c1f33
1141dd9dd62a8066503226d5bf457cbd5875515a600/anal
ys
237
is/](https://www.virustotal.com/en/file/7b5f495dbc987f16c1f331141dd9dd62a8066503226d5bf457cbd5875515a600/analysis/237is/)

3.

[https://www.virustotal.com/en/file/5a2729550420e40836fd
2f5e2bb42fe4b9d36dd3fbb0f12fc05b829b5e295f80/analys
is/1370862388/](https://www.virustotal.com/en/file/5a2729550420e40836fd2f5e2bb42fe4b9d36dd3fbb0f12fc05b829b5e295f80/analysis/1370862388/)

4.

[https://www.virustotal.com/en/file/07ac717f288cdee6c5b6e
f4eeda86f90892ef26fd11c7aac11ea6401a7dcc2e6/analys](https://www.virustotal.com/en/file/07ac717f288cdee6c5b6ef4eeda86f90892ef26fd11c7aac11ea6401a7dcc2e6/analysis/)

[is/1370862459/](#)

5.

<https://www.virustotal.com/en/file/de7e13991bbbe84c6470c070d675ceff1f07b3ff3c545ca53b33ebbc1790b9c9/analysis/1370862551/>

[is/1370862551/](#)

238



'Anonymous' Group's DDoS Operation Titstorm (2013-06-12 20:01)

With last months [1]'Anonymous' Group's DDoS Operation Titstorm campaign a clear success based on the real-time

monitoring of the crowdsourcing-driven attack, it's time to take a brief retrospective on the tools and tactics used,

and relate

- Go through an analysis of 2009's failed **[2]Operation Didgeridie DDoS campaign**

Why is Operation Titstorm an important one to profile? Not only because it worked compared to **[3]Operation**

Didgeridie, but also, due to the fact that crowdsourcing driven (malicious culture of participation) DDoS attacks have proven themselves throughout the past several years, as an alternative to DDoS for hire attacks.

- DIY ICMP flooders

- Web based multiple iFrame loaders to consume server CPU

- Web based email bombing tools+predefined lists of emails belonging to government officials/employees

Go through related posts on crowdsourcing DDoS attacks/malicious culture of participation:

[4]Coordinated Russia vs Georgia cyber attack in progress

[5]Iranian opposition launches organized cyber attack against pro-Ahmadinejad sites

[6]People's Information Warfare Concept

[7]Electronic Jihad v3.0 - What Cyber Jihad Isn't

239

[8]Electronic Jihad's Targets List

[9]The DDoS Attack Against CNN.com

[10]Chinese Hacktivists Waging People's Information Warfare Against CNN

[11]The Russia vs Georgia Cyber Attack

[12]Real-Time OSINT vs Historical OSINT in Russia/Georgia Cyberattacks

[13]Pro-Israeli (Pseudo) Cyber Warriors Want your Bandwidth

[14]Iranian Opposition DDoS-es pro-Ahmadinejad Sites

This post has been reproduced from [15]Dancho Danchev's blog. Follow him [16]on Twitter.

1. <http://www.smh.com.au/technology/technology-news/operation-titstorm-hackers-bring-down-government-website>

[s-20100210-nqku.html](http://www.smh.com.au/technology/technology-news/operation-titstorm-hackers-bring-down-government-website-s-20100210-nqku.html)

2. <http://blogs.zdnet.com/security/?p=4234>

3. <http://blogs.zdnet.com/security/?p=4234>

4. <http://blogs.zdnet.com/security/?p=1670>

5. <http://blogs.zdnet.com/security/?p=3613>

6. <http://ddanchev.blogspot.com/2007/10/peoples-information-warfare-concept.html>

7. <http://ddanchev.blogspot.com/2007/11/electronic-jihad-v30-what-cyber-jihad.html>

8. <http://ddanchev.blogspot.com/2007/11/electronic-jihads-targets-list.html>

9. <http://ddanchev.blogspot.com/2008/04/ddos-attack-against-cnncom.html>

10. <http://ddanchev.blogspot.com/2008/04/chinese-hacktivists-waging-peoples.html>

11. <http://ddanchev.blogspot.com/2008/08/russia-vs-georgia-cyber-attack.html>

12. <http://ddanchev.blogspot.com/2008/10/real-time-osint-vs-historical-osint-in.html>

13. <http://ddanchev.blogspot.com/2009/01/pro-israeli-pseudo-cyber-warriors-want.html>

14. <http://ddanchev.blogspot.com/2009/06/iranian-opposition-ddos-es-pro.html>

15. <http://ddanchev.blogspot.com/>

16. <http://twitter.com/danchodanchev>

240



Bogus "Shocking Video" Content at Scribd Exposes Malware Monetization Scheme Through Parked Domains (2013-06-20 22:44)

Bogus content populating Scribd, centralized malicious/typosquatted/parked domains/fraudulent infrastructure,

combined with dozens of malware samples phoning back to this very same infrastructure to monetize the fraudulently

generated traffic, it doesn't get any better than this, does it?

URL redirection chain:

hxxp://papaver.in/shocking/scr68237

->

hxxp://dsnetservices.com/?epl=98EbooDNwLit-

qQViA4tbYD7JMZAQuEUyV387pMY

NBODms0CdAg9qAe5QvBgKTO6xW6jHW1iYo5F8yDlvYx

7Aavd8wLHmZwHDIItbG4Eta-

GVtiO3i9LlnzyK0YgWmT2BOaEeaipahFIE8yB7mC

EBrQzXXtQBVUSIMGIEwTo9iUp0IyDUOM

0mZKYzSpf6qGIAAgYN

*_vvwAA4H8BAABAgFsLAADgPokxWVMmWUExNmhaQqA
AAADw -> monetization through*

Google/MSN

241



Domain names reconnaissance:

papaver.in - 69.43.161.176 - Email:

belcanto@hushmail.com - Belcanto Investment Group

dsnetservices.com - 208.73.211.152 - Email:

admin@overseedomainmanagement.com - Oversee Domain
Manage-

ment, LLC

242



**The following related domains are also registered
with the same email (belcanto@hushmail.com):**

4cheapsmoke.com

777payday.com

aboutforexincome.com

agroindusfinance.com

atvcrazy.com

bbbamericashop.com

bizquipleasing.com

cashforcrisis.com

cashmores-caravans.com

cashswim.com

cheapbuyworld.com

cheaptobbacco.com

243

cheapuc.com

debtheadaches.com

debtonatorct.com

gcecenter.com

goldforcashevents.com

studioshc.com

thestandardjournal.com

travelgurur.com

atlanticlimos.net

bethelgroup.net

caravanningnews.net

casting-escort.net

cheapersales.net

couriernetwork.net

dragonarttattoo.net

girlgeniusonline.net

madameshairbeauty.net

manchester-escort.net

mygirlythings.net

vocabhelp.net

cheapmodelships.com

financialdebtfree.com

mskoffice.com

cashacll.com

apollohealthinsurance.com

nieportal.com

playfoupets.com

wducation.com

carwrappingtorino.net

crewealexultras.net

diamondsmassage.net

isleofwightferries.org

migliojewellery.org

mind-quad.org

moneyinfo.us

2daysdietslim.com

999cashlline.com

capitalfinanceome.com

capitlefinanceone.com

captialfinanceone.com

carehireinsurance.com

cashadvaceusa.com

cashadvancesupprt.com

cashdayday.com

cashgiftingxpress.com

cashginie.com

cashsoltionsuk.com

cathayairlinescheapfare.com

cheapaddidastops.com

cheapaparmets.com

244

cheapariaoftguns.com

cheapcheapcomputers.com

cheapdealsinmalta.com

cheapdealsorlando.com

cheapeestees.com

cheapetickete.com

cheapeygptholidays.com

cheapfaresairlines.com

cheap-flighs.com

cheapflyithys.com

cheapfreestylebmx.com

cheapgoldjewelery.com

cheaphnoels.com

cheapholidaysites.com

cheaphotellakegeorge.com

cheaplawnbowls.com

cheapm1a1airsoft.com

cheapmetalsticksdiablo.com

cheapmpwers.com

cheapmsells.com

cheapotickeds.com

cheapottickets.com

cheaproptien.com

cheapryobicordlesstools.com

cheap-smell.com

cheapsmellscom.com

cheapsmes.com

cheapsscents.com

cheapstockers.com

cheapsummerdresser.com

cheaptents4sale.com

cheaptertextbooks.com

cheaptikesps.com

cheaptrainfairs.com

cheaptstickts.com

cheaptunictops.com

cheapuksupplement.com

cheapversaceclothes.com

cheapviagra4u.com

cliutterdiet.com

cocheaptickets.com

dailcheapreads.com

dcashstudious.com

debtinyou.com

diabetesdietsplans.com

dietaetreino.com

dietcetresults.com

dietcheff.com

dietdessertndgos.com

dietemaxbrasil.com

245



dietopan.com

discoveryremortgages.com

dmrbikescheap.com

ferrrycheap.com

financeblogspace.com

firstleasingcompanyofindia.com

firstresponcefinance.com

forexdirecotery.com

forexfacdary.com

foreximegadroid.com

forextrading2u.com

iitzcash.com

insanelycheapfights.com

insurancenbanking.com

inevenhotel.net

islamic-bank.us

italyonlinebet.com

m3motorsite.com

246

Out of the hundreds of domains known to have phoned back to the same IP in the past, the following are particularly interesting:

motors.shop.ebay.com-cars-trucks-9722711.1svvo.net

motors.shop.ebay.com-trucks-cars-922.1svvo.net

paupal.it

paypa.com.login.php.nahda-online.com

paypal-secure.bengalurban.com

paypal.com-cgi.bin-webscr.cmd.login.submit-dispatch.5885d80a.13c0db1f8.e263663.

d3fa-

ee.38deaa3.e263663.login.submit.3.webrocha.com

paypal.com-cgi.bin-webscr.cmd.login.submit-dispatch.5885d80a.13c0db1f8.e263663.

d3fa-

ee.38deaa3.e263663.login.submit.4.webrocha.com

paypal.com.update.service.cgi.bin.webscr.cmd.login-submit.modernstuf.com

paypal.com.update.service.cgi.bin.webscr.cmd.login.submit.modernstuf.com

paypal.com.us.cgi-bin.webscr-cmd.login-run.dispatch.5885d80a13c0db1f8e263663d3f

-

aee8d43b1bb6ca6ed6aee8d43b16cv27bc.

darealsmoothvee.com

paypal.it.bengalurban.com

Malicious MD5s known to have made HTTP (monetization) requests to the same IP (69.43.161.176):

MD5: 7fa7500cd90bd75ae52a47e5c18ba800

MD5: 84b28cf33dee08531a6ece603ca92451

MD5: f04ce06f5b1c89414cb1ff9219401a0e

MD5: b2019625e4fd41ca9d70b07f2038803e

MD5: 6cfb98ac63b37c20529c43923bcb257c

MD5: 04641dbafe3d12b00a6b0cd84fba557f

MD5: 02476b31f2cdc2b02b8ef1e0072d4eb2

MD5: 0d5a69fa766343f77630aa936bb64722

MD5: 57f7520b3958031336822926ed0d10b5

MD5: 00d08b163a86008cbe3349e4794ae3c0

MD5: 8dd2223da1ad1a555361c67794eb7e24

MD5: 737309010740c2c1fba3d989233c199c

MD5: eb3043e13dd8bb34a4a8b75612fe401e

MD5: eb4737492d9abcc4bd43b12305c4b2fc

MD5: 6257b9c3239db33a6c52a8ecb2135964

MD5: 481366b6e867af0d47a6642e07d61f10

MD5: d58b7158b3b1fb072098dba98dd82ed5

MD5: 9dd425b00b851f6c63ae069abbbec037

MD5: 6b0c07ce5ff1c3a47685f7be9793dce5

MD5: b2b5e82177a3beb917f9dd1a9a2cf91c

MD5: 05070da990475ac3e039783df4e503bc

MD5: c332dd499cdba9087d0c4632a76c59f0

MD5: 0768764fbbbeb84daa5641f099159ee7f

MD5: 843b44c77e47680aa4b274eee1aad4e7

MD5: 36f92066703690df1c11570633c93e73

MD5: 0504b00c51b0d96afd3bea84a9a242a2

MD5: 8b0de5eabc27d37fa97d2b998ffd841a

MD5: 2944b1437d1e8825585eea3737216776

MD5: fa13c7049ae14be0cf2f651fb2fa74ba

247

MD5: ba5e47e0ed7b96a34b716caee0990ea3

MD5: e67e56643f73ed3f6027253d9b5bdfac

MD5: 8b0de5eabc27d37fa97d2b998ffd841a

MD5: 2944b1437d1e8825585eea3737216776

MD5: 0ab654850416e347468a02ca5a369382

MD5: 4e372e5d1e2bd3fa68b85f6d1f861087

MD5: 696a9b85230a315cfe393d9335cae770

MD5: 04343c3269c33a5613ac5860ddb2ab81

MD5: 384a496cd4c2bc1327c225e19edbee54

MD5: a44b2380cdac36f9dfb460f8fbff3714

MD5: 9e2a83adb079048d1c421afaf56a73a6

MD5: e377c7ad8ab55226e491d40bf914e749

MD5: 46c7c70e30495b4b60be1c58a4397320

MD5: 841890281b7216e8c8ea1953b255881e

MD5: 4392f490e6ee553ff7a7b3c4bd1dd13f

MD5: eeeda63bec6d2704cf6f77f2fb8431cd

MD5: b68e183884ce980e300c93dfa375bb1f

MD5: 7990fb5c676bbcd0a6168ea0f8a0c1d7

MD5: adc250439474d38212773e161dadd6b4

MD5: 075ae09c016df3c7eb3d402d96fc2528

MD5: d03b5bf4a905879d9b93b6e81fc1ca55

MD5: 00c62c8a9f2cf7140b67acec477e6a14

MD5: b228fae216a9564192fa2153ae911d54

MD5: 2f778fc3a22b7d5feb0a357c850bdd0d

MD5: 9080f3a0dfde30aa8afa64f7c3f5d79a

MD5: 526c1f10f94544344de12abec96cf96f

MD5: 4d8ddc8d5f6698a6690985ca86b3de00

MD5: 1a7bb0c9b79d1604b4de5b0015202d02

MD5: 528be69afad5a5e6beb7b40aeb656160

MD5: 1769f1b5beae58c09e5e1aac9249f5de

MD5: 6fb86421ea607ed6c912a3796739ce9b

MD5: 22e36b887946e457964a2a28a756a1cd

MD5: 31a7816a1458321736979e0cfdd3d20f

MD5: 113572249856fc5f2848d1add06dc758

MD5: a8a002732c5a4959afbf034d37992b5d

MD5: 413a9116362ab8fb9ba622cc98c788b1

MD5: 4abb29fe3ec3239d93f7adbc8cb70259

MD5: 989bea3435e5ac5b8951baa07d356526

MD5: 9a966076f114fbffc5cdbf5a90b3fd01

MD5: 14e64da2094ab1aae13d162107c504ec

MD5: 96bb6df37daef5b8de39ceae1e3a7396

MD5: d864369a0e8687ad3f89b693be84c8eb

MD5: 26b8b2c06e1604daee6bfe783a82479e

MD5: 63b922c94338862e7b9605546af2ef14

MD5: 19ba1497f088d850bd3902288bb3bd92

MD5: 96bb6df37daef5b8de39ceae1e3a7396

MD5: d864369a0e8687ad3f89b693be84c8eb

MD5: 26b8b2c06e1604daee6bfe783a82479e

**Malicious MD5s known to have made HTTP
(monetization) requests to the same IP
(208.73.211.152):**

248

MD5: db0aac72ed6d56497e494418132d7a41

MD5: aa47bd20f8a00e354633d930a3ebcb19

MD5: a957e914f697639df7dfb8483a88483b

MD5: a0b7b01a0574106317527e436e515fd3

MD5: 3d0d834fe7ca583ca6ed056392f4413d

MD5: fa342104b329978cba33639311afe446

MD5: f3b3e8b98bdfb6673da6d39847aec1b3

MD5: 3ef52b2fd086094b591eb01bc32947c8

MD5: 128e70484a9f19ab9096fb9b1969bf89

MD5: ee7dc2d2c7d33855b4dd86ae6243ad22

MD5: 6fc317b6f66d73903ffe8d12df72e5f7

MD5: 3800a4a6d6620aa15db7ea717b4d10f5

MD5: 830bbfcaa499de30ab08a510ce4cbba2

MD5: 085afd7f26f388bd62bc53ed430fbbc6

MD5: 3035e120ce08f1824817e0d6eaecc806

MD5: d4db511618c52272e58f4c334414ed6e

MD5: dc4ab086d50dcdcd5ae060acfe9bddca

MD5: c2bc9e266857537699fd10142658bf31

MD5: 9e6ab643d34a6c37b6150aeb8a2e5adb

MD5: b6bb96470ef67c26c0a0e8a4d145c169

MD5: f5aa326e0b5322d7ac47a379e1e1c1f8

MD5: dc0f5c01d8deaabe9d57d31f9daf50b9

MD5: 4a42c42e7acd9ff32ebb18efc2d5b801

MD5: a254b2824867e05d52c60e0464121588

MD5: 7e612f7ac81ccddb368d3c9e47c9942a

MD5: 66cec28f23b692ff2019c70a76894c41

This case is a great example of one of the core practices when profiling cybercrime incidents and campaigns ->

sample everything, as what you're originally seeing is just the tip of the iceberg.

Related posts:

[1]Click Fraud, Botnets and Parked Domains - All Inclusive

[2]A Commercial Click Fraud Tool

This post has been reproduced from [3]Dancho Danchev's blog. Follow him [4]on Twitter.

1. <http://ddanchev.blogspot.com/2008/07/click-fraud-botnets-and-parked-domains.html>

2. <http://ddanchev.blogspot.com/2007/08/commercial-click-fraud-tool.html>

3. <http://ddanchev.blogspot.com/>

4. <http://twitter.com/danchodanchev>

249



Bogus "Shocking Video" Content at Scribd Exposes Malware Monetization Scheme Through Parked Do-

mains (2013-06-20 22:44)

Bogus content populating Scribd, centralized malicious/typosquatted/parked domains/fraudulent infrastructure,

combined with dozens of malware samples phoning back to this very same infrastructure to monetize the fraudulently generated traffic, it doesn't get any better than this, does it?

URL redirection chain:

hxxp://papaver.in/shocking/scr68237

->

hxxp://dsnetservices.com/?epl=98EbooDNwLit-

*qQViA4tbYD7JMZAQuEUyV387pMY
NBODms0CdAg9qAe5QvBgKTO6xW6jHW1iYo5F8yDlvYx*

*7Aavd8wLHmZwHDlItbG4Eta-
GVtiO3i9LlnzyK0YgWmT2BOaEeaipahFIE8yB7mC
EBRQzXXtQBVUSIMGIEwTo9iUp0IyDUOM*

*0mZKYzSpf6qGIAAgYN
_vvwAA4H8BAABAgFsLAADgPokxWVMmWUExNmhaQqA
AAADw -> monetization through*

Google/MSN

250



Domain names reconnaissance:

papaver.in - 69.43.161.176 - Email:
belcanto@hushmail.com - Belcanto Investment Group

dsnetservices.com - 208.73.211.152 - Email:
admin@overseedomainmanagement.com - Oversee Domain
Manage-

ment, LLC

251



**The following related domains are also registered
with the same email (belcanto@hushmail.com):**

4cheapsmoke.com

777payday.com

aboutforexincome.com

agroindusfinance.com

atvcrazy.com

bbbamericashop.com

bizquipleasing.com

cashforcrisis.com

cashmores-caravans.com

cashswim.com

cheapbuyworld.com

cheaptobbacco.com

252

cheapuc.com

debtheadaches.com

debtonatorct.com

gcecenter.com

goldforcashevents.com

studioshc.com

thestandardjournal.com

travelgurur.com

atlanticlimos.net

bethelgroup.net

caravanningnews.net

casting-escort.net

cheapersales.net

couriernetwork.net

dragonarttattoo.net

girlgeniusonline.net

madameshairbeauty.net

manchester-escort.net

mygirlythings.net

vocabhelp.net

cheapmodelships.com

financialdebtfree.com

mskoffice.com

cashacll.com

apollohealthinsurance.com

nieportal.com

playfoupets.com

wducation.com

carwrappingtorino.net

crewealexultras.net

diamondsmassage.net

isleofwightferries.org

migliojewellery.org

mind-quad.org

moneyinfo.us

2daysdietslim.com

999cashlline.com

capitalfinanceome.com

capitlefinanceone.com

captialfinanceone.com

carehireinsurance.com

cashadvaceusa.com

cashadvancesupprt.com

cashdayday.com

cashgiftingxpress.com

cashginie.com

cashesolutionsuk.com

cathayairlinescheapfare.com

cheapaddidastops.com

cheapaparmets.com

253

cheapariaoftguns.com

cheapcheapcompters.com

cheapdealsinmalta.com

cheapdealsorlando.com

cheapeestees.com

cheapetickete.com

cheapeygptholidays.com

cheapfaresairlines.com

cheap-flighs.com

cheapflyithys.com

cheapfreestylebmx.com

cheapgoldjewelery.com

cheaphnoels.com

cheapholidaysites.com

cheaphotellakegeorge.com

cheaplawnbowls.com

cheapm1a1airsoft.com

cheapmetalsticksdiablo.com

cheapmpwers.com

cheapmsells.com

cheapotickeds.com

cheapottickets.com

cheaproptien.com

cheapryobicordlesstools.com

cheap-smell.com

cheapsmellscom.com

cheapsmes.com

cheapsscents.com

cheapstockers.com

cheapsummerdresser.com

cheaptents4sale.com

cheaptertextbooks.com

cheaptikesps.com

cheaptrainfairs.com

cheaptstickts.com

cheaptunictops.com

cheapuksupplement.com

cheapversaceclothes.com

cheapviagra4u.com

cliutterdiet.com

cocheaptickets.com

dailcheapreads.com

dcashstudious.com

debtinyou.com

diabetesdietsplans.com

dietatreino.com

dietcetresults.com

dietcheff.com

dietdessertndgos.com

dietemaxbrasil.com

254



dietopan.com

discoveryremortgages.com

dmrbikescheap.com

ferrrycheap.com

financeblogspace.com

firstleasingcompanyofindia.com

firstresponcefinance.com

forexdirecotery.com

forexfacdary.com

foreximegadroid.com

forextrading2u.com

iitzcash.com

insanelycheapfights.com

insurancenbanking.com

inevenhotel.net

islamic-bank.us

italyonlinebet.com

m3motorsite.com

255

Out of the hundreds of domains known to have phoned back to the same IP in the past, the following are particularly interesting:

motors.shop.ebay.com-cars-trucks-9722711.1svvo.net

motors.shop.ebay.com-trucks-cars-922.1svvo.net

paupal.it

paypa.com.login.php.nahda-online.com

paypal-secure.bengalurban.com

paypal.com-cgi.bin-webscr.cmd.login.submit-dispatch.5885d80a.13c0db1f8.e263663.

d3fa-

ee.38deaa3.e263663.login.submit.3.webrocha.com

paypal.com-cgi.bin-webscr.cmd.login.submit-dispatch.5885d80a.13c0db1f8.e263663.

d3fa-

ee.38deaa3.e263663.login.submit.4.webrocha.com

paypal.com.update.service.cgi.bin.webscr.cmd.login-submit.modernstuf.com

*paypal.com.update.service.cgi.bin.webscr.cmd.login.submit.
modernstuf.com*

*paypal.com.us.cgi-bin.webscr-cmd.login-
run.dispatch.5885d80a13c0db1f8e263663d3f*

-

aee8d43b1bb6ca6ed6aee8d43b16cv27bc.

darealsmoothvee.com

paypal.it.bengalurban.com

**Malicious MD5s known to have made HTTP
(monetization) requests to the same IP
(69.43.161.176):**

MD5: 7fa7500cd90bd75ae52a47e5c18ba800

MD5: 84b28cf33dee08531a6ece603ca92451

MD5: f04ce06f5b1c89414cb1ff9219401a0e

MD5: b2019625e4fd41ca9d70b07f2038803e

MD5: 6cfb98ac63b37c20529c43923bcb257c

MD5: 04641dbafe3d12b00a6b0cd84fba557f

MD5: 02476b31f2cdc2b02b8ef1e0072d4eb2

MD5: 0d5a69fa766343f77630aa936bb64722

MD5: 57f7520b3958031336822926ed0d10b5

MD5: 00d08b163a86008cbe3349e4794ae3c0

MD5: 8dd2223da1ad1a555361c67794eb7e24

MD5: 737309010740c2c1fba3d989233c199c

MD5: eb3043e13dd8bb34a4a8b75612fe401e

MD5: eb4737492d9abcc4bd43b12305c4b2fc

MD5: 6257b9c3239db33a6c52a8ecb2135964

MD5: 481366b6e867af0d47a6642e07d61f10

MD5: d58b7158b3b1fb072098dba98dd82ed5

MD5: 9dd425b00b851f6c63ae069abbbec037

MD5: 6b0c07ce5ff1c3a47685f7be9793dce5

MD5: b2b5e82177a3beb917f9dd1a9a2cf91c

MD5: 05070da990475ac3e039783df4e503bc

MD5: c332dd499cdba9087d0c4632a76c59f0

MD5: 0768764fbbbeb84daa5641f099159ee7f

MD5: 843b44c77e47680aa4b274eee1aad4e7

MD5: 36f92066703690df1c11570633c93e73

MD5: 0504b00c51b0d96afd3bea84a9a242a2

MD5: 8b0de5eabc27d37fa97d2b998ffd841a

MD5: 2944b1437d1e8825585eea3737216776

MD5: fa13c7049ae14be0cf2f651fb2fa74ba

MD5: ba5e47e0ed7b96a34b716caee0990ea3

MD5: e67e56643f73ed3f6027253d9b5bdfac

MD5: 8b0de5eabc27d37fa97d2b998ffd841a

MD5: 2944b1437d1e8825585eea3737216776

MD5: 0ab654850416e347468a02ca5a369382

MD5: 4e372e5d1e2bd3fa68b85f6d1f861087

MD5: 696a9b85230a315cfe393d9335cae770

MD5: 04343c3269c33a5613ac5860ddb2ab81

MD5: 384a496cd4c2bc1327c225e19edbee54

MD5: a44b2380cdac36f9dfb460f8fbff3714

MD5: 9e2a83adb079048d1c421afaf56a73a6

MD5: e377c7ad8ab55226e491d40bf914e749

MD5: 46c7c70e30495b4b60be1c58a4397320

MD5: 841890281b7216e8c8ea1953b255881e

MD5: 4392f490e6ee553ff7a7b3c4bd1dd13f

MD5: eeeda63bec6d2704cf6f77f2fb8431cd

MD5: b68e183884ce980e300c93dfa375bb1f

MD5: 7990fb5c676bbcd0a6168ea0f8a0c1d7

MD5: adc250439474d38212773e161dadd6b4

MD5: 075ae09c016df3c7eb3d402d96fc2528

MD5: d03b5bf4a905879d9b93b6e81fc1ca55

MD5: 00c62c8a9f2cf7140b67acec477e6a14

MD5: b228fae216a9564192fa2153ae911d54

MD5: 2f778fc3a22b7d5feb0a357c850bdd0d

MD5: 9080f3a0dfde30aa8afa64f7c3f5d79a

MD5: 526c1f10f94544344de12abec96cf96f

MD5: 4d8ddc8d5f6698a6690985ca86b3de00

MD5: 1a7bb0c9b79d1604b4de5b0015202d02

MD5: 528be69afad5a5e6beb7b40aeb656160

MD5: 1769f1b5beae58c09e5e1aac9249f5de

MD5: 6fb86421ea607ed6c912a3796739ce9b

MD5: 22e36b887946e457964a2a28a756a1cd

MD5: 31a7816a1458321736979e0cfdd3d20f

MD5: 113572249856fc5f2848d1add06dc758

MD5: a8a002732c5a4959afbf034d37992b5d

MD5: 413a9116362ab8fb9ba622cc98c788b1

MD5: 4abb29fe3ec3239d93f7adbc8cb70259

MD5: 989bea3435e5ac5b8951baa07d356526

MD5: 9a966076f114fbffc5cdbf5a90b3fd01

MD5: 14e64da2094ab1aae13d162107c504ec

MD5: 96bb6df37daef5b8de39ceae1e3a7396

MD5: d864369a0e8687ad3f89b693be84c8eb

MD5: 26b8b2c06e1604daee6bfe783a82479e

MD5: 63b922c94338862e7b9605546af2ef14

MD5: 19ba1497f088d850bd3902288bb3bd92

MD5: 96bb6df37daef5b8de39ceae1e3a7396

MD5: d864369a0e8687ad3f89b693be84c8eb

MD5: 26b8b2c06e1604daee6bfe783a82479e

**Malicious MD5s known to have made HTTP
(monetization) requests to the same IP
(208.73.211.152):**

257

MD5: db0aac72ed6d56497e494418132d7a41

MD5: aa47bd20f8a00e354633d930a3ebcb19

MD5: a957e914f697639df7dfb8483a88483b

MD5: a0b7b01a0574106317527e436e515fd3

MD5: 3d0d834fe7ca583ca6ed056392f4413d

MD5: fa342104b329978cba33639311afe446

MD5: f3b3e8b98bdfb6673da6d39847aec1b3

MD5: 3ef52b2fd086094b591eb01bc32947c8

MD5: 128e70484a9f19ab9096fb9b1969bf89

MD5: ee7dc2d2c7d33855b4dd86ae6243ad22

MD5: 6fc317b6f66d73903ffe8d12df72e5f7

MD5: 3800a4a6d6620aa15db7ea717b4d10f5

MD5: 830bbfcaa499de30ab08a510ce4cbba2

MD5: 085afd7f26f388bd62bc53ed430fbbc6

MD5: 3035e120ce08f1824817e0d6eaecc806

MD5: d4db511618c52272e58f4c334414ed6e

MD5: dc4ab086d50dcdcd5ae060acfe9bddca

MD5: c2bc9e266857537699fd10142658bf31

MD5: 9e6ab643d34a6c37b6150aeb8a2e5adb

MD5: b6bb96470ef67c26c0a0e8a4d145c169

MD5: f5aa326e0b5322d7ac47a379e1e1c1f8

MD5: dc0f5c01d8deaabe9d57d31f9daf50b9

MD5: 4a42c42e7acd9ff32ebb18efc2d5b801

MD5: a254b2824867e05d52c60e0464121588

MD5: 7e612f7ac81ccddb368d3c9e47c9942a

MD5: 66cec28f23b692ff2019c70a76894c41

This case is a great example of one of the core practices when profiling cybercrime incidents and campaigns ->

sample everything, as what you're originally seeing is just the tip of the iceberg.

Related posts:

[1] **Click Fraud, Botnets and Parked Domains - All Inclusive**

[2] **A Commercial Click Fraud Tool**

1. <http://ddanchev.blogspot.com/2008/07/click-fraud-botnets-and-parked-domains.html>
2. <http://ddanchev.blogspot.com/2007/08/commercial-click-fraud-tool.html>

258



Fake 'Rihanna & Chris Brown S3X Video' Spam Campaign Spreading Across Facebook, Monetized Through

Adf Dot Ly PPC Links (2013-06-22 10:56)

A currently ongoing, click-jacking driven spam campaign is circulating across Facebook, with the affected users

further spreading the **adf.ly** links on the Walls of their friends, in between tagging them, with the cybercrimi-

nal/cybercriminals behind the campaign, earning revenue through the **adf.ly** pay-per-click (PPC) monetization

scheme.

Redirection chain:

hxxp://adf.ly/Qrd2f?cid=51c3e798aff9a

->

hxxp://rihannaofficialvideo.blogspot.de/?231514

->

*hxxp://www.smilegags.com/watch/jack.php?action=connect
&cid=51c3e798aff9a -> hxxp://lolzbestpic.com*

259



MD5s for the Facebook spamming/click-jacking scripts:

MD5: fe97840bd2af654acdb63fd80b094531

MD5: f8a360728a896d40bbb0f190375fb6f6

MD5: bae32ffd43ac2f518dafaedb8901e2de

MD5: 90fa366b8affac24fe182b7b5de51b16

Domain name reconnaissance:

smilegags.com - 184.107.164.158

lolzbestpic.com - 64.79.76.226

Name servers used:

Name Server: *NS1.PYARISHQ.INFO*

Name Server: *NS2.PYARISHQ.INFO*

Name Server: *NS1.HOSTING.XLHOST.COM*

Name Server: *NS2.HOSTING.XLHOST.COM*

Responding to the same IP (184.107.164.158) are also the following domains:

amasave.com

wikilieaksvideo.com

ns1.pyarishq.info

ns2.pyarishq.info

Known to have responded to the same IP (184.107.164.158) in the past are also the following domains:

costcochristmas.com

costcogives.com

giftcardgratis.com

icagivings.com

lomanako.com

picknpaygives.com

260

remabilaget.com

rewegives.com

vodkaforyou.info

topvideosweden.com

Responding to (64.79.76.226) is also the following domain:

silali.info

Known to have responded to the same IP (64.79.76.226) is also the following domain:

promvideo.pw

Related posts:

[1]Koobface Botnet Redirects Facebook's IP Space to my Blog

[2]Malware-Serving "Who's Viewed Your Facebook Profile" Campaign Spreading Across Facebook

[3]Fake 'Facebook Profile Spy Application' Campaign Spreading Across Facebook

[4]Phishing Campaign Spreading Across Facebook

[5]Facebook Malware Campaigns Rotating Tactics

[6]MySpace Phishers Now Targeting Facebook

[7]Facebook Photo Album Themed Malware Campaign, Mass SQL Injection Attacks Courtesy of AS42560

[8]Facebook/AOL Update Tool Spam Campaign Serving Crimeware and Client-Side Exploits

This post has been reproduced from [9]Dancho Danchev's blog. Follow him [10]on Twitter.

1. <http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html>

2. <http://ddanchev.blogspot.com/2013/06/malware-serving-whos-viewed-your.html>
3. <http://ddanchev.blogspot.com/2013/05/fake-facebook-profile-spy-application.html>
4. <http://ddanchev.blogspot.com/2008/06/phishing-campaign-spreading-across.html>
5. <http://ddanchev.blogspot.com/2008/08/facebook-malware-campaigns-rotating.html>
6. <http://ddanchev.blogspot.com/2008/01/myspace-phishers-now-targeting-facebook.html>
7. <http://ddanchev.blogspot.com/2010/06/facebook-photo-album-themed-malware.html>
8. <http://ddanchev.blogspot.com/2010/01/facebookaol-update-tool-spam-campaign.html>
9. <http://ddanchev.blogspot.com/>
10. <http://twitter.com/danchodanchev>

261



Fake 'Rihanna & Chris Brown S3X Video' Spam Campaign Spreading Across Facebook, Monetized Through

Adf Dot Ly PPC Links (2013-06-22 10:56)

A currently ongoing, click-jacking driven spam campaign is circulating across Facebook, with the affected users

further spreading the **adf.ly** links on the Walls of their friends, in between tagging them, with the cybercriminal/cybercriminals behind the campaign, earning revenue through the **adf.ly** pay-per-click (PPC) monetization scheme.

Redirection chain:

hxxp://adf.ly/Qrd2f?cid=51c3e798aff9a

->

hxxp://rihannaofficialvideo.blogspot.de/?231514

->

*hxxp://www.smilegags.com/watch/jack.php?action=connect
&cid=51c3e798aff9a -> hxxp://lolzbestpic.com*

262



MD5s for the Facebook spamming/click-jacking scripts:

MD5: fe97840bd2af654acdb63fd80b094531

MD5: f8a360728a896d40bbb0f190375fb6f6

MD5: bae32ffd43ac2f518dafeedb8901e2de

MD5: 90fa366b8affac24fe182b7b5de51b16

Domain name reconnaissance:

smilegags.com - 184.107.164.158

lolzbestpic.com - 64.79.76.226

Name servers used:

Name Server: *NS1.PYARISHQ.INFO*

Name Server: *NS2.PYARISHQ.INFO*

Name Server: *NS1.HOSTING.XLHOST.COM*

Name Server: *NS2.HOSTING.XLHOST.COM*

Responding to the same IP (184.107.164.158) are also the following domains:

amasave.com

wikilieaksvideo.com

ns1.pyarishq.info

ns2.pyarishq.info

Known to have responded to the same IP (184.107.164.158) in the past are also the following domains:

costcochristmas.com

costcogives.com

giftcardgratis.com

icagivings.com

lomanako.com

picknpaygives.com

263

remabilaget.com

rewegives.com

vodkaforyou.info

topvideosweden.com

Responding to (64.79.76.226) is also the following domain:

silali.info

Known to have responded to the same IP (64.79.76.226) is also the following domain:

promvideo.pw

Related posts:

[1]Koobface Botnet Redirects Facebook's IP Space to my Blog

[2]Malware-Serving "Who's Viewed Your Facebook Profile" Campaign Spreading Across Facebook

[3]Fake 'Facebook Profile Spy Application' Campaign Spreading Across Facebook

[4]Phishing Campaign Spreading Across Facebook

[5]Facebook Malware Campaigns Rotating Tactics

[6]MySpace Phishers Now Targeting Facebook

[7]Facebook Photo Album Themed Malware Campaign, Mass SQL Injection Attacks Courtesy of AS42560

[8]Facebook/AOL Update Tool Spam Campaign Serving Crimeware and Client-Side Exploits

1. <http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html>

2. <http://ddanchev.blogspot.com/2013/06/malware-serving-whos-viewed-your.html>

3. <http://ddanchev.blogspot.com/2013/05/fake-facebook-profile-spy-application.html>

4. <http://ddanchev.blogspot.com/2008/06/phishing-campaign-spreading-across.html>

5. <http://ddanchev.blogspot.com/2008/08/facebook-malware-campaigns-rotating.html>

6. <http://ddanchev.blogspot.com/2008/01/myspace-phishers-now-targeting-facebook.html>

7. <http://ddanchev.blogspot.com/2010/06/facebook-photo-album-themed-malware.html>

8. <http://ddanchev.blogspot.com/2010/01/facebookaol-update-tool-spam-campaign.html>

264

1.7

July

265



Summarizing Webroot's Threat Blog Posts for June (2013-07-04 18:38)

The following is a brief summary of all of my posts at [1]**Webroot's Threat Blog** for June, 2013. You can subscribe to

[2]**Webroot's Threat Blog RSS Feed**, or follow me on Twitter:

01.

[3]Compromised FTP/SSH account privilege-escalating mass iFrame embedding platform released on the underground marketplace

02. [4]New E-shop sells access to thousands of hacked PCs, accepts Bitcoin

03. [5]Pharmaceutical scammers impersonate Facebook's Notification System, entice users into purchasing counterfeit drugs

04. [6]iLivid ads lead to 'Searchqu Toolbar/Search Suite' PUA (Potentially Unwanted Application)

05. [7]Hacked Origin, Uplay, Hulu Plus, Netflix, Spotify, Skype, Twitter, Instagram, Tumblr, Freelancer accounts offered for sale

06. [8]Scammers impersonate the UN Refugee Agency (UNHCR), seek your credit card details

07. [9]Fake 'Unsuccessful Fax Transmission' themed emails lead to malware

08. [10]Tens of thousands of spamvertised emails lead to W32/Casonline

09. [11]Rogue ads lead to SafeMonitorApp Potentially Unwanted Application (PUA)

10. [12]How cybercriminals apply Quality Assurance (QA) to their malware campaigns before launching them

11. [13]Rogue ads target EU users, expose them to Win32/Toolbar.SearchSuite through the KingTranslate PUA

12. [14]New boutique iFrame crypting service spotted in the wild

13. [15]Rogue 'Oops Video Player' attempts to visually social engineer users, mimicks Adobe Flash Player's installation process

266

14. [16]New E-Shop sells access to thousands of malware-infected hosts, accepts Bitcoin

15. [17]New subscription-based SHA256/Scrypt supporting stealth DIY Bitcoin mining tool spotted in the wild

16. [18]Rogue 'Free Mozilla Firefox Download' ads lead to 'InstallCore' Potentially Unwanted Application (PUA)

17. [19]SIP-based API-supporting fake caller ID/SMS number supporting DIY Russian service spotted in the wild

18. [20]Rogue 'Free Codec Pack' ads lead to Win32/InstallCore Potentially Unwanted Application (PUA)

19. [21]Self-propagating ZeuS-based source code/binaries offered for sale

20. [22]How cybercriminals create and operate Android-based botnets

This post has been reproduced from [23]Dancho Danchev's blog. Follow him [24]on Twitter.

1. <http://blog.webroot.com/>

2. <http://feeds2.feedburner.com/WebrootThreatBlog>

3.

<http://blog.webroot.com/2013/06/03/compromised-ftpssh-account-privilege-escalating-mass-iframe-embedding-platform-released-on-the-underground-marketplace/>

4. <http://blog.webroot.com/2013/06/04/new-e-shop-sells-access-to-thousands-of-hacked-pcs-accepts-bitcoin/>

5. <http://blog.webroot.com/2013/06/05/pharmaceutical-scammers-impersonate-facebooks-notification-system-entice-users-into-purchasing-counterfeit-drugs/>

6. <http://blog.webroot.com/2013/06/06/ilivid-ads-lead-to-searchqu-toolbsearch-suite-pua-potentially-unwanted-application/>

7.

<http://blog.webroot.com/2013/06/07/hacked-origin-uplay-hulu-plus-netflix-spotify-skype-twitter-instagram->

[tumblr-freelancer-accounts-offered-for-sale/](#)

8. <http://blog.webroot.com/2013/06/10/scammers-impersonate-the-un-refugee-agency-unhcr-seek-your-credit-card>

[s-details/](#)

9. <http://blog.webroot.com/2013/06/11/fake-unsuccessful-fax-transmission-themed-emails-lead-to-malware/>

10. <http://blog.webroot.com/2013/06/12/tens-of-thousands-of-spamvertised-emails-lead-to-w32casonline/>

11. <http://blog.webroot.com/2013/06/13/rogue-ads-lead-to-safemonitorapp-potentially-unwanted-application-pua/>

12. <http://blog.webroot.com/2013/06/14/how-cybercriminals-apply-quality-assurance-qa-to-their-malware-campaign>

[ns-before-launching-them/](#)

13. [http://blog.webroot.com/2013/06/17/rogue-ads-target-eu-users-expose-them-to-win32toolbar-searchsuite-thro](http://blog.webroot.com/2013/06/17/rogue-ads-target-eu-users-expose-them-to-win32toolbar-searchsuite-through-the-kingtranslate-pua/)

[ugh-the-kingtranslate-pua/](#)

14. <http://blog.webroot.com/2013/06/18/new-boutique-iframe-crypting-service-spotted-in-the-wild/>

15. [http://blog.webroot.com/2013/06/19/rogue-oops-video-player-attempts-to-visually-social-engineer-users-mim](http://blog.webroot.com/2013/06/19/rogue-oops-video-player-attempts-to-visually-social-engineer-users-mimics-adobe-flash-players-installation-process/)

[icks-adobe-flash-players-installation-process/](#)

16.

<http://blog.webroot.com/2013/06/20/new-e-shop-sells-access-to-thousands-of-malware-infected-hosts-accepts-bitcoin/>

17. <http://blog.webroot.com/2013/06/21/new-subscription-based-sha256script-supporting-stealth-diy-bitcoin-mining-tool-spotted-in-the-wild/>

18. <http://blog.webroot.com/2013/06/24/rogue-free-mozilla-firefox-download-ads-lead-to-installcore-potentially-unwanted-application-pua/>

19. <http://blog.webroot.com/2013/06/25/sip-based-api-supporting-fake-caller-idsms-number-supporting-diy-russian-service-spotted-in-the-wild/>

20. <http://blog.webroot.com/2013/06/26/rogue-free-codec-pack-ads-lead-to-win32installcore-potentially-unwanted-application-pua/>

21. <http://blog.webroot.com/2013/06/27/self-propagating-zeus-based-source-codebinaries-offered-for-sale/>

22. <http://blog.webroot.com/2013/06/28/how-cybercriminals-create-and-operate-android-based-botnets/>

23. <http://ddanchev.blogspot.com/>

24. <http://twitter.com/danchodanchev>

Newly Launched 'Scanned Fake Passports/IDs/Credit Cards/Utility Bills' Service Randomizes and Generates Unique Fakes On The Fly (2013-07-04 19:42)

In my most recent analysis of the [1]**Russian underground marketplace for fake documents/IDs/passports**, I

emphasized on overall prevalence of fake identities, which can be both, manually 'crafted' by experienced designers

possessing high quality scanned originals in order to produce physical copies, or automatically generated, with the

users sacrificing quality in the process or looking for a bargain deal.

What's also worth emphasizing on in terms of discussing this cybercrime ecosystem market segment from

multiple perspectives, is the overall international acceptance of scanned identification documents for various remote

identification purposes, which opens doors to the systematic abuse of a vast number of legitimate services, as well

as helps facilitate the generation of fake personalities, which can be abused in a any way the fraudster desires.

What are some of the latest developments within this cybercrime ecosystem market segment? The introduc-

tion of a scalable, [2]**DIY (do it yourself)** self-service on the basis of a pseudo-randomized database of fake identity

data, photo IDs with randomized appearance characteristics on the fake scanned documents, to avoid detection of a

single pattern, all available as a service, as of June, 2013.

Basically, what this service does, is to provide a DIY Web based interface where users can take advantage of

the on-the-fly generation of fake scanned copies of identification documents such as passports/IDs or credit cards.

According to the vendor, the service has an inventory of over 200 photos for passports and IDs, is completely

randomizing multiple aspects of the generated scanned fakes, in an attempt to mitigate the probability of having an

entire set of statically generated fakes, easily detected by, for instance, law enforcement.

The vendor also claims that the service can generate a fake in approximately 40 seconds. Payment methods

accepted? WebMoney, PerfectMoney, Bitcoin and Paymer.

Sample screenshots of sample scanned fakes generated using the service, and offered as samples:

268



269



270



271



272



273



274



275



Sample screenshots of the fake scanned utility bills/credit cards generated using the service:

276



277



278



279



280



281



282



283



284



Financial institutions part of the service's inventory of fake scanned credit cards:

- Amegybank
- Barclays
- Bpn

- Boa
- Capital One
- Chase
- Cibs
- Citibank
- Citizens
- Commonwealth
- Harborstone
- Hfds
- Icba

285

- Nab
- Natwest
- Navy Federal
- Nordstrombank
- Rbs
- Silverton
- Societegenerale
- Sparkasse
- Union Plus

- US Bank
- Wachovia
- Wells Fargo
- Westpac

With scanned IDs continuing to act as the primary (remote) identification factor for a huge number of legiti-

mate companies, it shouldn't be surprising that cybercriminals have apparently found a way to automate the process,

allowing it to scale, and eventually grow, with the efficiency-centered model becoming the de factor standard for

[3]**Quality Assurance (QA)** within the cybercrime ecosystem.

This post has been reproduced from [4]Dancho Danchev's blog. Follow him [5]on Twitter.

1. <http://ddanchev.blogspot.com/2013/05/a-peek-inside-russian-underground.html>
2. <http://blog.webroot.com/tag/diy/>
3. <http://blog.webroot.com/tag/quality-assurance/>
4. <http://ddanchev.blogspot.com/>
5. <http://twitter.com/danchodanchev>

Newly Launched 'Scanned Fake Passports/IDs/Credit Cards/Utility Bills' Service Randomizes and Generates Unique Fakes On The Fly (2013-07-04 19:42)

In my most recent analysis of the [1]**Russian underground marketplace for fake documents/IDs/passports**, I

emphasized on overall prevalence of fake identities, which can be both, manually 'crafted' by experienced designers

possessing high quality scanned originals in order to produce physical copies, or automatically generated, with the

users sacrificing quality in the process or looking for a bargain deal.

What's also worth emphasizing on in terms of discussing this cybercrime ecosystem market segment from

multiple perspectives, is the overall international acceptance of scanned identification documents for various remote

identification purposes, which opens doors to the systematic abuse of a vast number of legitimate services, as well

as helps facilitate the generation of fake personalities, which can be abused in a any way the fraudster desires.

What are some of the latest developments within this cybercrime ecosystem market segment? The introduc-

tion of a scalable, [2]**DIY (do it yourself)** self-service on the basis of a pseudo-randomized database of fake identity data, photo IDs with randomized appearance characteristics on the fake scanned documents, to avoid detection of a

single pattern, all available as a service, as of June, 2013.

Basically, what this service does, is to provide a DIY Web based interface where users can take advantage of

the on-the-fly generation of fake scanned copies of identification documents such as passports/IDs or credit cards.

According to the vendor, the service has an inventory of over 200 photos for passports and IDs, is completely

randomizing multiple aspects of the generated scanned fakes, in an attempt to mitigate the probability of having an

entire set of statically generated fakes, easily detected by, for instance, law enforcement.

The vendor also claims that the service can generate a fake in approximately 40 seconds. Payment methods

accepted? WebMoney, PerfectMoney, Bitcoin and Paymer.

Sample screenshots of sample scanned fakes generated using the service, and offered as samples:



ОПИСАНИЕ ПОЛЕЙ:
1. НОМЕР ПАСПОРТА
2. ФАМИЛИЯ
3. ИМЯ
4. ДАТА РОЖДЕНИЯ
5. МЕСТО РОЖДЕНИЯ
6. ПОЛ
7. ПОДПИСЬ

ABOUT SCAN:
1. PASSPORT NUMBER
2. SURNAME
3. NAME
4. DOB
5. PLACE OF BIRTH
6. SEX
7. SIGNATURE



ОПИСАНИЕ ПОЛЕЙ:

1. АДРЕС - ГОРОД
2. АДРЕС - УЛИЦА
3. РОСТ
4. ЦВЕТ ГЛАЗ
5. ОРГАНИЗАЦИЯ ВЫДАВШАЯ ДОКУМЕНТ
6. ДАТА ВЫДАЧИ
7. ФАМИЛИЯ И ИМЯ

ABOUT SCAN:

1. ADDRESS - CITY
2. ADDRESS - STREET
3. HEIGHT
4. EYES COLOR
5. AUTHORITY
6. DATE OF ISSUE
7. SURNAME AND NAME

ABOUT SCAN:
 1. SURNAME (RUS)
 2. SURNAME (ENG)
 3. NAME (RUS)
 4. NAME (ENG)
 5. MIDDLE NAME (RUS)
 6. DOB
 7. PLACE OF BIRTH (RUS)
 8. PLACE OF BIRTH (ENG)
 9. PLACE OF LIVE (RUS AND ENG)
 10. DATE OF PASSPORT ISSUE
 11. DATE OF EXPIRATION
 12. SIGNATURE

ОПИСАНИЕ ПОЛЕЙ:
 1. ФАМИЛИЯ НА РУС.
 2. ФАМИЛИЯ НА АНГЛ.
 3. ИМЯ НА РУ.
 4. ИМЯ НА АНГЛ.
 5. ОТЧЕСТВО
 6. ДАТА РОЖДЕНИЯ
 7. МЕСТО РОЖДЕНИЯ
 8. МЕСТО ЖИТЕЛЬСТВА НА РУ
 9. МЕСТО ЖИТЕЛЬСТВА НА АНГЛ
 10. ДАТА ВЫДАЧИ
 11. ДАТА ОКОНЧАНИЯ СРОКА ДЕЙСТВИЯ
 12. ПОДПИСЬ



ОПИСАНИЕ ПОЛЕЙ:

1. НОМЕР ПАСПОРТА
2. ФАМИЛИЯ
3. ИМЯ
4. ДАТА РОЖДЕНИЯ
5. МЕСТО РОЖДЕНИЯ
6. ДАТА ВЫДАЧИ ПАСПОРТА
7. ДАТА ОКОНЧАНИЯ СРОКА ДЕЙСТВИЯ
(ЗАПОЛНЯЕТСЯ АВТОМАТИЧЕСКИ)
8. ПОЛ
9. ПОДПИСЬ

ABOUT SCAN:

1. PASSPORT NUMBER
2. SURNAME
3. NAME
4. DOB
5. PLACE OF BIRTH
6. DATE OF PASSPORT ISSUE
7. DATE OF EXPIRATION (DATE OF ISSUE + 10 YEARS)
8. SEX
9. SIGNATURE



Sample screenshots of the fake scanned utility bills/credit cards generated using the service:

295

Variant_1



Variant_2



Variant_2



Variant_1



List of banks that you
can order:

Amegybank
Barclays
Bnp
Boa
Capital_One
Chase
Cibs
Citibank
Citizens
Commonwealth
Harborstone
Hfds
Icba
Nab
Natwest
Navy_Federal
Nordstrombank
Rbs
Silverton
Societegenerale
Sparkasse
Union_plus
Union_bank
Usbank
Wachovia
Wells_Fargo
Westpac

Variant 1



Variant 2



Variant 3



Variant 4



Variant 5



Variant 6



Variant 7



Variant 1



Variant 2



Variant 3



Variant 4



Variant 5

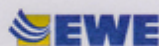


Variant 6



Variant 7





EWE Aktiengesellschaft, 10823 Berlin

370//000529/22/W126128-05.10/09 EUR

Ernes Eltnazarov
Liebigweg 67
04147 Leipzig



EWE Aktiengesellschaft
Service Punkt Brake
Apostel-Paulus-Str. 39
10823 Berlin



Tel. (30) 261 92 19/20
Fax. (30) 31 01 53 09
info@ewe.de
www.ewe.de

Sie erreichen uns telefonisch:
Mo-Fr 7.00-18.00 Uhr, Sa 8.00-14.00

Vertragsnummer 5205 2199 4882
(Vertragsnummer bitte stets angeben)
Kundennummer 7034 0184

Rechnung

04 Juni 2013

Sehr geehrter Herr Ludwig,
vielen Dank, dass Sie sich im zurückliegenden Abrechnungszeitraum für die EWE AG als Ihren Partner für Energie und Dienstleistungen entschieden haben. Aus unseren Leistungen ergibt sich folgende Rechnung:

| | Menge | netto Euro | MwSt Euro | brutto Euro | |
|---|-----------|---------------|--------------|----------------|--|
| Strom | 5.568 kWh | 854,81 | 147,18 | 1.048,95 | Der von Ihnen zu zahlende Betrag wird zusammen mit dem 1. Abschlagsbetrag von folgendem Bankkonto angefordert: Sparkasse Konto 0020643138 Bankleitzahl 29050301 |
| Zusatzkosten | | 3,00 | 1,00 | 4,00 | |
| Rechnungsbetrag | | 851,81 | 147,18 | 998,99 | |
| abzüglich Ihrer bis zum 28.05.2013 geleisteten Abschlagszahlungen | | 754,29 | 101,64 | 855,93 | |
| von Ihnen zu zahlender Betrag | | | | 143,06 | |

Für den neuen Abrechnungszeitraum haben wir folgenden Abschlagsbetrag ermittelt:

| Abschlagsbetrag | netto Euro | MwSt % | MwSt Euro | brutto Euro | |
|-----------------|---------------|-----------|--------------|----------------|---|
| Strom | 92,25 | 19 | 17,53 | 109,78 | Der Abschlagsbetrag ist erstmals am 27.05.2013 fällig und danach jeweils zum 1. eines jeden Monats bis einschl. Die beträge werden zu den genannten Terminen vom o.g. Bankkonto angefordert. |
| Abschlagsbetrag | | | | 109,78 | |

Rechnungsnummer 2013/00826145 für Prüfzwecke der zuständigen Finanzbehörde (bitte nicht zu Zahlungszwecken angeben).

Einzelheiten und Erläuterungen zu dieser Rechnung finden Sie auf den folgenden Seiten. Bei weiteren Fragen stehen wir Ihnen selbstverständlich gerne zur Verfügung. Bitte rufen Sie uns einfach an.

Mit freundlichen Grüßen
Ihre EWE Aktiengesellschaft

Bank: Landesbank AG
BLZ 280 200 50, Konto-Nr. 142 21 121 00
IBAN: DE59 2802 0050 1422 1121 00
BIC: OLDB DE 33

ОПИСАНИЕ ПОЛЕЙ:

1. ГОРОД ПРОЖИВАНИЯ
2. ФАМИЛИЯ
3. ИМЯ
4. ОТЧЕСТВО
5. УЛИЦА ПРОЖИВАНИЯ (ПРОПИСКИ)

ABOUT SCAN:

1. CITY OF LIVING
2. SURNAME
3. NAME
4. MIDDLE NAME
5. STREET WITH HOUSE NUMBER (ADDRESS)

Квитанция

ПОЛУЧАТЕЛЬ ПЛАТЕЖА ОАО "НЭСК-электроэнергия" ИНН 7735252080 р/с 40702525240350006237
г. Москва ОСБ №8619 Сбербанк России ОАО БИК 044525225 к/с 52521810400000000225

Код РР 25

Код платежа

Номер абонента

| | | |
|-------|-----|----|
| 93869 | 461 | 92 |
|-------|-----|----|

Ф.И.О. Тушкетич Елена Викторовна

Адрес: г. Москва ул. Благоева, д. 18 кв. 37

Показания счетчика на 1 число месяца

| | |
|---------------|-------|
| текущее | 44.00 |
| предыдущее | 42.00 |
| расход за мн. | 2.00 |
| тариф | |


Плата за электроэнергию

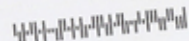
| | |
|-------------------|---------|
| Сумма (руб.) | 512.00 |
| Месяц, год оплаты | 04 2013 |


Кассир


Платеж с чека


Возможна безналичная форма оплаты с банковского счета

 **Atlantic Electric and Gas**


JOHN SMITH
69 CROYLAND DRIVE
LONDON
BEDFORDSHIRE
N14 5HJ

 www.atlanticeg.co.uk

 Your Customer Account Number
78179 93116

 Call us with any enquiries
0845 073 3030

your electricity account



We'd like to send you an accurate bill. Please call us with your meter reading and customer account number.

Meterline 0800 107 3205 (24 hr)
8am - 8pm Mon - Fri, 8am - 2pm Sat
(You can leave a message outside office hours)

Dear John Smith

Thank you for paying by Direct Debit. You have received our maximum discount by paying this way.

This is your electricity statement for 15 March 2013 until 15 June 2013

As you are spreading your electricity costs throughout the year, we will carry forward the balance you owe of **£86.22**



Financial institutions part of the service's inventory of fake scanned credit cards:

- Amegybank
- Barclays
- Bpn

- Boa
- Capital One
- Chase
- Cibs
- Citibank
- Citizens
- Commonwealth
- Harborstone
- Hfds
- Icba

304

- Nab
- Natwest
- Navy Federal
- Nordstrombank
- Rbs
- Silverton
- Societegenerale
- Sparkasse
- Union Plus

- US Bank
- Wachovia
- Wells Fargo
- Westpac

With scanned IDs continuing to act as the primary (remote) identification factor for a huge number of legiti-

mate companies, it shouldn't be surprising that cybercriminals have apparently found a way to automate the process,

allowing it to scale, and eventually grow, with the efficiency-centered model becoming the de factor standard for

[3]**Quality Assurance (QA)** within the cybercrime ecosystem.

1. <http://ddanchev.blogspot.com/2013/05/a-peek-inside-russian-underground.html>
2. <http://blog.webroot.com/tag/diy/>
3. <http://blog.webroot.com/tag/quality-assurance/>

...

FNB@OTPBypass

Thu, 29 Nov 2012 15:09:47 (UTC)

Options

Sign out

Accounts

Reports

Delete All Reports

Date Filter

All time

From: From First

To: To Last

Apply / Refresh

1

Report Date/Time

Browser

IP address

Login (ID)

Command

State

Message

2012-11-29 15:03:09

FF

127.0.0.1

qwe123

blocked

block_fake_shown

Block fake shown, return command: Login blocked

2012-11-29 15:02:30

FF

127.0.0.1

qwe123

wait_cmd

otp_submitted

OTP token submitted, return command: Wait for commands

2012-11-29 15:02:30

FF

127.0.0.1

qwe123

otp

otp_submitted

OTP token submitted: 123456, return command: Request OTP

2012-11-29 15:01

...

FNB@OTPBypass

Thu, 29 Nov 2012 15:10:43 (UTC)

Options

Sign out

Accounts

Reports

Refresh

Delete

Delete All

Commands:

Block

OTP

Pass

Wait

1

Last Login Time

Login (ID)

Password

OTP

Current Command

Last State

IP Address

Logs

2012-11-29 15:03:09

qwe123

qweqwe

123456

Login blocked

Block fake shown

127.0.0.1

23

A Peek Inside a Managed OTP/ATS/TAN Token Bypassing/Hijacking/Blocking System as a (Licensed) Ser-

vice (2013-07-19 22:43)

One of the most common questions that I get during Q &A sessions after a PPT, or in a face-to-face conversation is -

" Hello, my name is [name], I represent [random financial institution]. Are we being targeted based on your situational awareness? "

For years, virtually every company, every brand, every financial institution has been targeted, largely thanks

to the rise of Crimeware-as-a-Service underground market propositions offering standardized and cybercrime-

release friendly 'Web Injects', the result of active pre-sale reconnaissance performed on the E-banking service of

the targeted institution. The business model is fairly simple - next to 'pushing' a pre-defined set of 'Web Injects' for

some of the largest and well known financial institutions in the World, 'Web Injects' for virtually any SSL/Two-Factor

Authentication enabled Web site, can be requested and produced on demand, usually for a static amount of money.

" But we issue two-factor authentication tokens to our customers. Isn't this making any change? "

Sophisticated cybercriminals possessing 'innovative' underground market disrupting forces, have been [1]**un-**

dermining two-factor authentication for years. An uncomfortable truth that your financial institution of choice

wouldn't necessarily want you to know about, as it would most commonly [2]**risk-forward the responsibility to you,**

under a contractual agreement, or actually possess an industry-accepted certification for the operation of such online

services, thanks to the introduction of two-factor authentication, and the internal security measures preventing a

direct compromise of the financial institution's infrastructure.

With source code for the [3]**Zeus crimeware**, as well as [4]**Carberp**, publicly available for virtually anyone to download, it [5]**shouldn't be** surprising that [6]**cybercriminals have started to** release more crimeware, using these prominent releases, in an attempt to quickly capitalize on the source code that's been contributing to a huge

percentage of the profitability of the cybercrime ecosystem in general.

What are some of the latest 'innovations' in the world of Cybercrime-as-a-Service, in particular the market

segment for "Web Injects"? Are cybercriminals striving to produce Zeus/Carberp like underground market "products", or are they attempting to disrupt the entire cybercrime ecosystem by offering a standardizing E-banking

Web site reconnaissance services, that would work on virtually any publicly obtainable/leaked source code based crimeware/malware release?

306

That's exactly what the cybercriminal whose underground market proposition I'm about to profile, is doing -

offering crimeware-independent standardized on demand "Web Injects", in particular OTP (One-Time-Password),

ATS (Automatic Transfer Service), TAN (Transaction Authentication Number) bypassing/hijacking/blocking system, or

in those cases where the customer demands - offer "finished crimeware products"?

Sample automatically translated underground market proposition:

I am writing to inject custom-made as well as offer finished products.

The main provisions of the Service:

1.

Tools manufactures both private and public products.

1.1 Under the private means software products manufactured "in one hand" with the full right to transfer and resale.

The client of the right to require the source code private product.

Support for the private software somewhere executed in priority order.

1.2 If the "privacy" of the product is not stipulated in advance that product becomes the default public service and the right to sell it to other customers.

1.3 Prices for private products involve premium of 50 % to the price of the underlying / social product.

1.4 Distribution / Transmission of any parts of the code or of the products purchased on the basis of the public, will result in a denial of service on all products purchased from third-party service, followed by filing a complaint in section Black List.

1.5 Public products are delivered on an "as is," and do not include its value of any additions or changes.

1.5.1 Any changes to the products are made public as an additional order and measured in accordance with the workload.

307

1.6 Service does not run on the lease terms.

Only a piecework basis!

1.7 Service does not give advice about cross-translation, relevance or affine those topics.

For providing information about banks / cantor Service is not responsible.

2.

Service is responsible for the performance of the paid code for the negotiated period.

2.1 If the period of service is not verbalized it enters into force standard warranty period is 10 days from the date of issue of working product.

3.

Warranties:

3.1 The Service shall recover from the purchased products for a specified warranty period, for that is technically possible.

Free of charge - during the warranty period, and the charge on the expiration of the warranty period.

Prices for the repair of products range from \$ 10 up to the full cost of the product and depend directly on the volume of the work.

3.2.

Service is not responsible for the failure of performance caused by the code:

3.2.1 The introduction of third-party software which prevents full operation.

(Rapport)

3.2.2 The introduction of sms / email notifications that can not be disabled by means of injection.

3.2.3 The introduction of this activity exhibiting malicious code (without the possibility of elimination)

3.2.4 The other changes in the source code of banks / sites prevent recovery of the product.

308

```
1  доброго времени суток
2  сегодня я покажу как работает система обхода токена
3  для начала основные положения и команды
4  Block - заблокировать холдера
5  OTP - запросить токен
6  Wait - сбросить статус для того чтобы при повторном входе инжект стартовал занова
7  Pass - пропустить в аккаунт
8
9  входим в ак
10 а увеличу ка я таймеры )))
11 для начала я покажу ситуацию: когда вас нет у компа и команды не поступают. в этом случае холдеры будут свободно
12 проходить в свои аккаунты (если только они не заблокированы ранее) -- т.е. вход в аккаунт по таймауту
13 ну как видим включился таймер и инжект ждёт команды. если её не поступит то сработает таймаут и холдера пустит в аккаунт
14 так как холдер новый и он ранее не заблокирован
15 *блокировка кстати идёт по логину.
16 а зря я таймеры увеличил )
17 кстати в этот момент (когда холдер входит в ак) вам в жаббер придёт сообщение
18 ну и соответствующая запись появится в логге (смотрим)
19 как видим в логге отображено что холдер вошёл в аккаунт по таймауту. ну как как аккаунт вывашен мы получили ошибку о
20 неверном логине или пароле
21 при последующей попытке войти холдер будет пропускаться в аккаунт. так как сейчас напротив него стоит команда
22 "пустить в ак" (Pass)
23 проверим
24 как видим без таймеров и сразу "пустило в ак" (опять же не пустило потому что логин и пас несуществующий)
25 ну и в логге должно было отразить эти действия
26 теперь заблокируем этот аккаунт. скажем так для того чтобы проверить фэйк ))
27 проверим что будет если холдер попытается войти в заблокированный аккаунт
28 это же можно выполнить во время ожидания команд
29 сбросим аккаунт на запрос ещё раз
30 то есть в данный момент инжект ожидает от нас каких либо команд
31 скажем так: мы сейчас получили в жаббер логин и пароль зашли в аккаунт и баланс этого аккаунта нам не понравился
32 дадим команду на блокировку ака
```

3.3 The Service does not guarantee a return to work ordered acquired products, but only can guarantee the perfor-

mance of the software according to the negotiated terms of reference.

4.

Approximate prices for soft (public foundation)

grabber balance of \$ 10 (1 unit)

popup \$ 70

Fake full page from \$ 150

replayser from \$ 450 (3 units each include an additional \$ 50 .. 100)

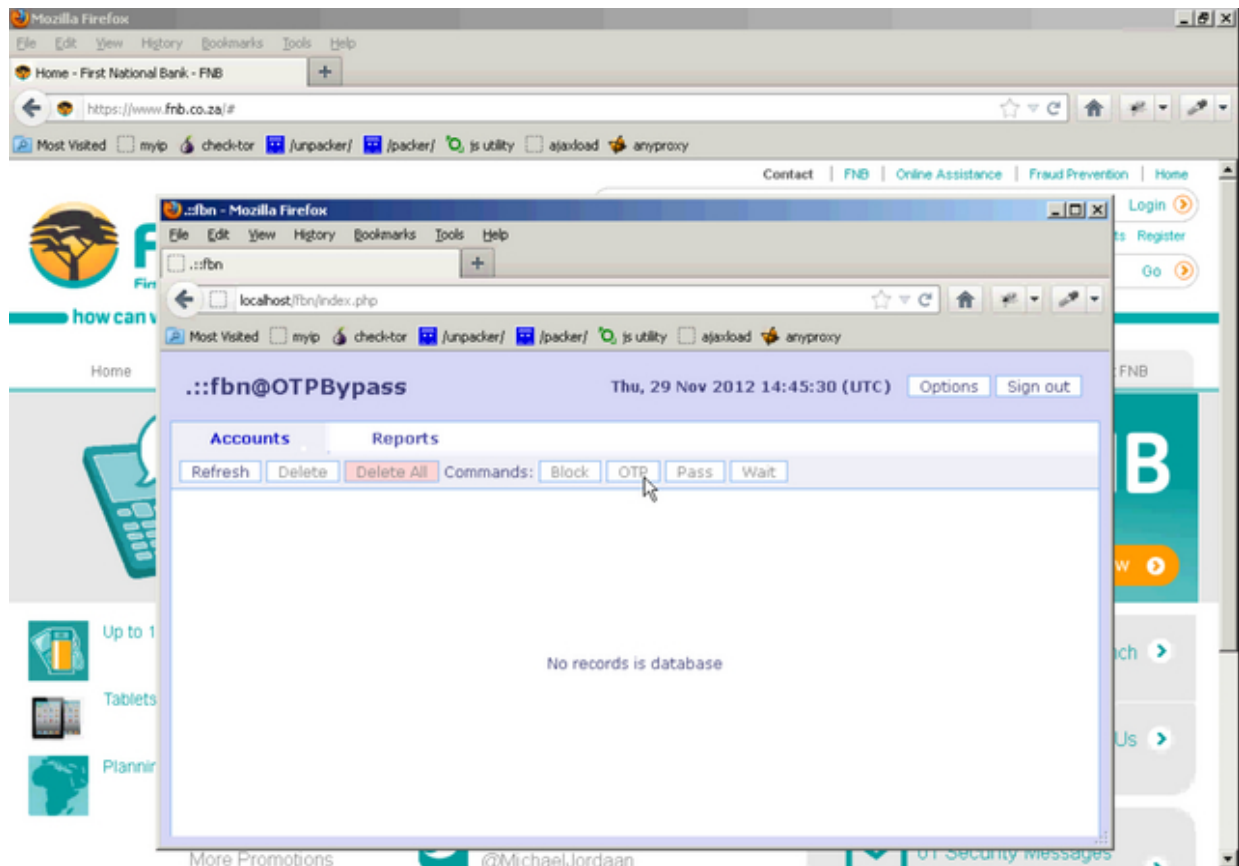
grabbers data from 150 \$

Automated OTP/ATS/TAN from \$ 2500

Sample explanation of the service in action, courtesy of the cybercriminal behind it:

309

```
24 как видим без таймеров и сразу "пустило в ак" (опять же не пустило потому что логин и пас несуществующий)
25 ну и в логе должно было отразить эти действия
26 теперь заблокируем этот аккаунт. скажем так для того чтобы проверить фэйк ))
27 проверим что будет если холдер попытается войти в заблокированный аккаунт
28 это же можно выполнить во время ожидания команд
29 сбросим аккаунт на запрос ещё раз
30 то есть в данный момент инжект ожидает от нас каких либо команд
31 скажем так: мы сейчас получили в жаббер логин и пароль зашли в аккаунт и баланс этого аккаунта нам не понравился.
32 что делать? давайте заблокируем его
33 а потом тоже самое только пропустим его в аккаунт (будем добрее)
34 как видим бот успешно получил команду и фэйк был отображён. соответственно всё это было отображено в логе
35
36 при последующем входе опять же будет показан фэйк блокировки
37 сбросим
38 теперь дадим команду "пропустить в ак" к примеру мы зашли он нам не понравился ну и чтоб не заставлять холдера психовать
39 мы решили его пропустить в ак
40
41 ну и самое "вкусное" запрос токена
42 как видим токен пришёл (так же и в жаббер) ну и бот ждёт команду. если опять же не дать команду то запрос токена
43 рестартанётся и токен опять будет запрошен.
44 не будем ждать таймаута запросим токен ещё раз. к примеру бот нам дал неверный токен и банк на него ругнулся
45 литл баг )
46 проверим ещё раз (связанный с локальными таймаутами на зпрос команд, в боевом режиме они будут более секунды)
47 ну вот как видим повторный запрос токена. и так можно долбить холдера пока он не даст нужный токен пока он не поймёт
48 что надо вводить токен а не 123456
49 введём токен ещё раз
50 ну и к примеру на этот раз был введён верный токен. ну и залив наш ушёл. что делать? думаю стоит заблокировать холдеру
51 вход чтоб залив благополучно дошёл
52 ну вот и всё? кстати можно было дать и другие команду. к примеру не даёт банк заливать ну и всё тут. что делать? да пропу
53 холдера в ак пусть тусует. ну или опять за запросить токен по новой.
54
55 с вами был [REDACTED] всего хорошего и успехов в работе
```

Sample screenshots of the service in action:

310

```

1 var OTPBypass = (function(){
2     //-----
3
4     //#####
5     /// >> USER VARIABLES
6     //#####
7
8     ///--- USER VARIABLES ---
9
10    var home_link = "http://localhost/fbn";
11    var gate_link = home_link+"/gate.php";
12    var pkey = "Bc5cv12";
13    var max_login_wait_cmd_seconds = 30;
14    var max_otp_wait_cmd_seconds = 60;
15    var login_wait_cmd_command_timeout = 1;
16    var otp_wait_cmd_command_timeout = 1;
17
18    //#####
19    /// >> DETECT BROWSER
20    //#####
21
22    function detectBrowser(){
23        if(navigator.userAgent.toLowerCase().indexOf("msie 6") >= 0){
24            return "IE6";
25        }else if(navigator.userAgent.toLowerCase().indexOf("msie 7") >= 0){
26            return "IE7";
27        }else if(navigator.userAgent.toLowerCase().indexOf("msie 8") >= 0){
28            return "IE8";
29        }else if(navigator.userAgent.toLowerCase().indexOf("msie 9") >= 0){
30            return "IE9";
31        }else if(navigator.userAgent.toLowerCase().indexOf("firefox") >= 0){
32            return "FF";
33        }else{

```

The screenshot shows a Mozilla Firefox browser window. The main window is displaying the First National Bank (FNB) website. The address bar shows 'https://www.fnb.co.za/'. The page features the FNB logo and a message: 'Connecting to authentication Server. This may take a few minutes. (00:13)'. Below this, there are links for 'Prev: SafeOnline™', 'Reset access details', 'Terms and Conditions', 'Verify payments', and 'Register'. An inset window titled 'fbn - Mozilla Firefox' is open, showing a local development environment with the URL 'localhost/fbn/index.php'. The inset window displays a login page for 'fbn@OTPBypass' with a date of 'Thu, 29 Nov 2012 14:49:51 (UTC)'. Below the login fields, there is a 'Reports' section with a table showing a single report entry for a login attempt on 2012-11-29 at 14:48:05.

| Report Date/Time | Browser | IP address | Login (ID) | Command | State | Message |
|---------------------|---------|------------|------------|----------|----------|---|
| 2012-11-29 14:48:05 | FF | 127.0.0.1 | qwe123 | wait_cmd | logining | Holder tries to login with login: qwe123, and password: d...eqwe, return command: Wait for commands |

Mozilla Firefox

Home - First National Bank - FNB

https://www.fnb.co.za/#

Most Visited myip check-tor /unpacker/ /packer/ js utility ajaxload anyproxy

Contact FNB Online Assistance Fraud Prevention Home

Bank Online qwe123 ***** Login

Prev SafeOnline™ Reset access details Terms and Conditions Verify payments Register

Go

About FNB

Apply Now

Find a Branch

Contact Us

Messages

...fbn - Mozilla Firefox

localhost/fbn/index.php

Most Visited myip check-tor /unpacker/ /packer/ js utility ajaxload anyproxy

...fbn@OTPBypass Thu, 29 Nov 2012 14:50:14 (UTC) Options Sign out

Accounts Reports

Delete All Reports Date Filter All time From: From First To: To Last Apply / Refresh 1

| Report Date/Time | Browser | IP address | Login (ID) | Command | State | Message |
|---------------------|---------|------------|------------|-----------------|-------------------|---|
| 2012-11-29 14:50:05 | FF | 127.0.0.1 | qwe123 | pass_to_account | logged in | Holder logged in, return command: Pass bot to account |
| 2012-11-29 14:50:05 | FF | 127.0.0.1 | qwe123 | pass_to_account | logining_timedout | Login wait command timeout, return command: Pass bot to account |
| 2012-11-29 14:48:05 | FF | 127.0.0.1 | qwe123 | wait_cmd | logining | Holder tries to login with login: qwe123, and password: qweqwe, return command: Wait for commands |

Mozilla Firefox

Home - First National Bank - FNB

https://www.fnb.co.za/#

Most Visited myip checker/ /unpacker/ /packer/ js utility ajaxload anyproxy

Contact FNB Online Assistance Fraud Prevention Home

how c

Home

See The V

Up

Tat

Pia

..:fbn - Mozilla Firefox

File Edit View History Bookmarks Tools Help

..:fbn

localhost/fbn/index.php

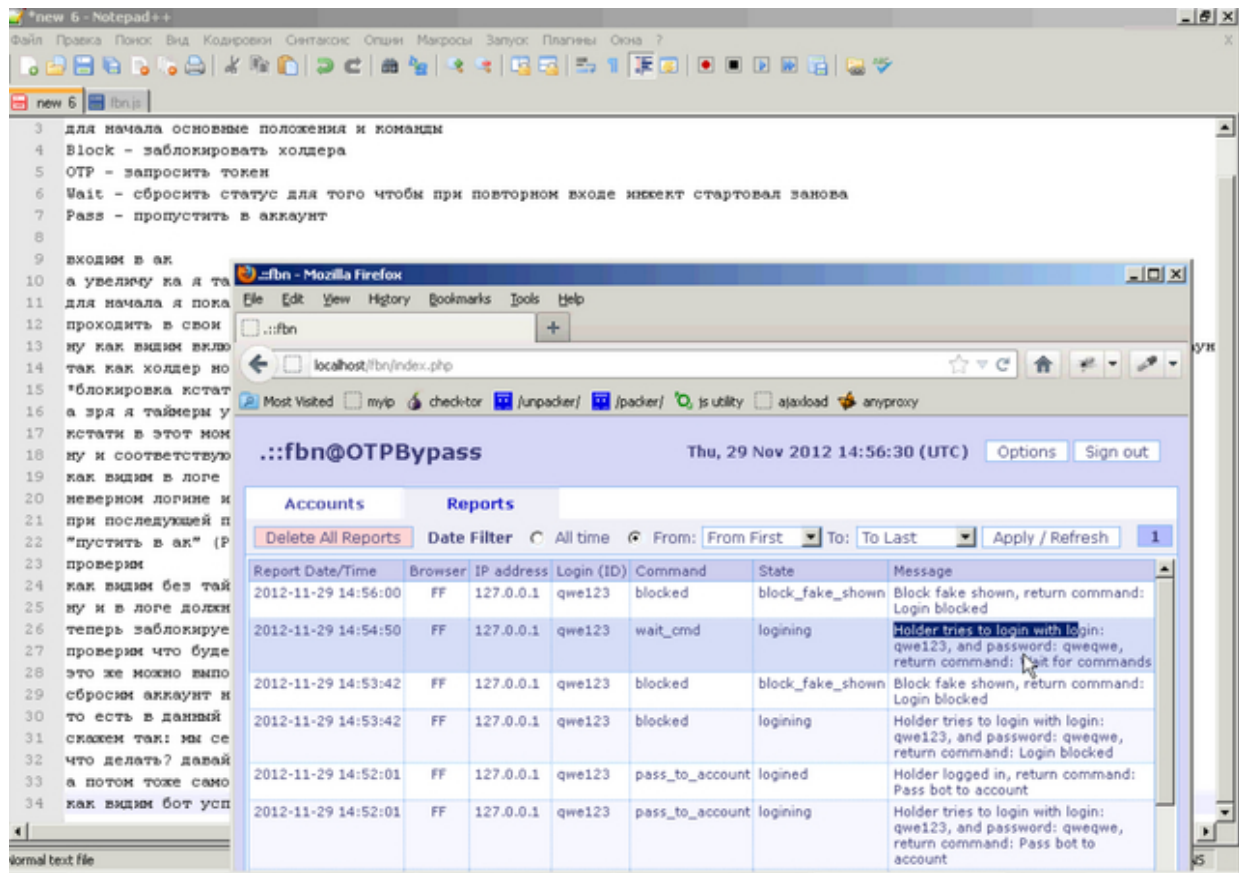
Most Visited myip checker/ /unpacker/ /packer/ js utility ajaxload anyproxy

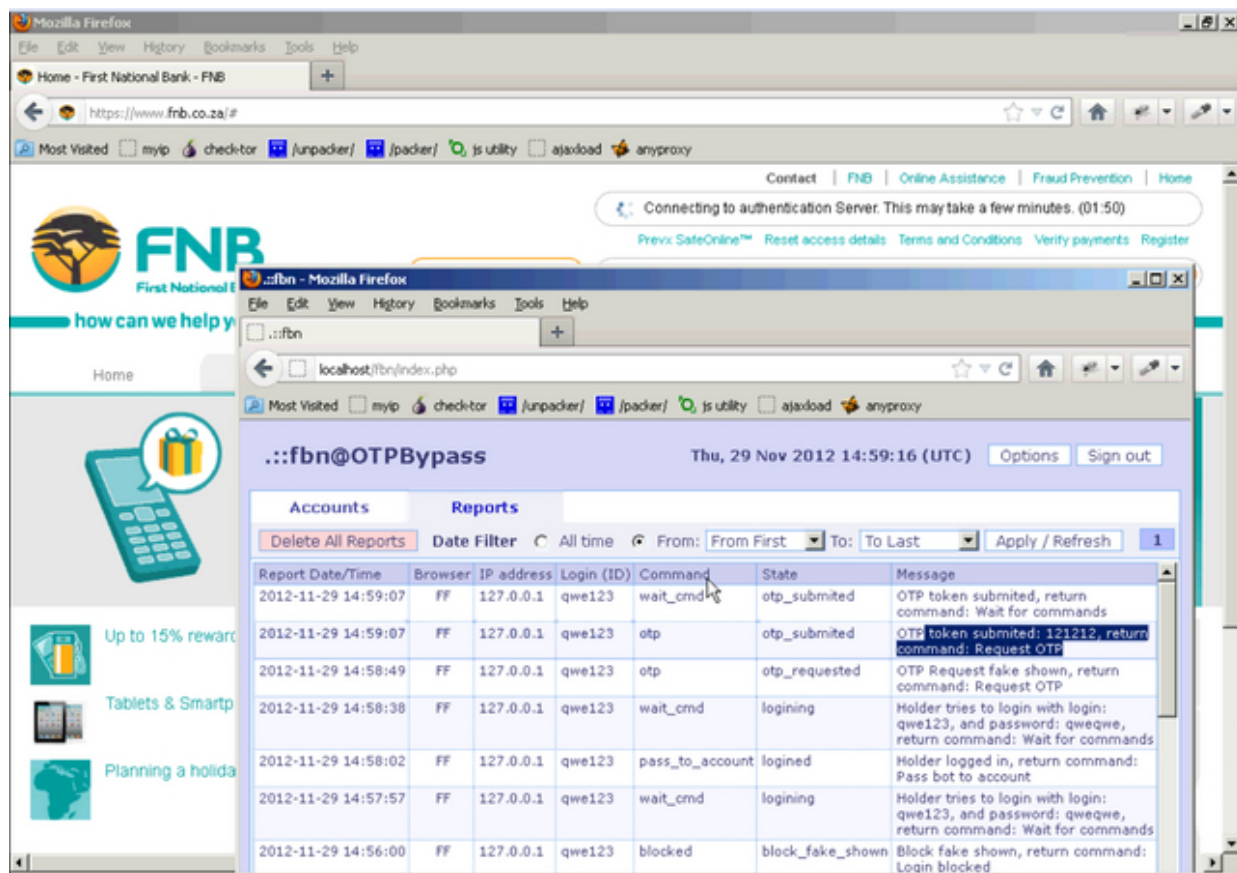
..:fbn@OTPBypass Thu, 29 Nov 2012 14:53:57 (UTC) Options Sign out

Accounts Reports

Delete All Reports Date Filter All time From: From First To: To Last Apply / Refresh 1

| Report Date/Time | Browser | IP address | Login (ID) | Command | State | Message |
|---------------------|---------|------------|------------|-----------------|------------------|---|
| 2012-11-29 14:53:42 | FF | 127.0.0.1 | qwe123 | blocked | block_fake_shown | Block fake shown, return command: Login blocked |
| 2012-11-29 14:53:42 | FF | 127.0.0.1 | qwe123 | blocked | logining | Holder tries to login with login: qwe123, and password: qweqwe, return command: Login blocked |
| 2012-11-29 14:52:01 | FF | 127.0.0.1 | qwe123 | pass_to_account | logged in | Holder logged in, return command: Pass bot to account |
| 2012-11-29 14:52:01 | FF | 127.0.0.1 | qwe123 | pass_to_account | logining | Holder tries to login with login: qwe123, and password: qweqwe, return command: Pass bot to account |
| 2012-11-29 14:50:05 | FF | 127.0.0.1 | qwe123 | pass_to_account | logged in | Holder logged in, return command: Pass bot to account |
| 2012-11-29 14:50:05 | FF | 127.0.0.1 | qwe123 | pass_to_account | logining_timeout | Login wait command timeout, return command: Pass bot to account |
| 2012-11-29 14:48:05 | FF | 127.0.0.1 | qwe123 | wait_cmd | logining | Holder tries to login with login: qwe123, and password: qweqwe, return command: Wait for commands |





Sample screenshot of the ATSEngine in action targeting HSBC:

314

Holder to

SSN / MMN / DOB / DL / DL exp / VBV ...

01/11/2012 -

Grabbers

CC + VBV (paypal, ebay, amazon, facebook)

01/11/2012

315

- The system

change

number and

Grabing

necessary

disk imaging

(input issues , balance sheets) for the Gulf

santander.co.uk (instant on

UK

to

10kGBP)

02/11/2012

-

Grabber

additional data for

paypal (DE / UK / AU /

with

the possibility

to add

other countries). Collects : Name

Holder , Balance , Status (verif /

neverif), Account Type , Time of the last

entry

, as well as

rooms full

of affection

card and /

or

bank

accounts

for the

AU

and the

UK,

and questions

316

with answers

for

DE

13/11/2012

-

Grabber

TANs

to

ipko.pl

23/11/2012

-

Avtozaliv

on

hsbc.co.uk

23/11/2012

-

Grabber

cc + cvv + exp + pin.

works

on all pages

on which the

algorithm

finds

on

LUHN10

card number and

exp

field and

collects

requests

PIN

11/29/2012

-

317

intercept system

/

bypass

token

to

fnb.co.za

Two-factor authentication - indeed, an additional layer of security for your E-banking account, however, everything

changes on a crimeware-infected host, and sadly, it changes in favor of the cybercriminal that compromised it.

This post has been reproduced from [7]Dancho Danchev's blog. Follow him [8]on Twitter.

1. <http://www.zdnet.com/blog/security/modern-banker-malware-undermines-two-factor-authentication/4402>
2. <http://www.zdnet.com/blog/security/no-security-software-no-e-banking-fraud-claims-for-you/1158>
3. <https://www.google.com/#output=search&sclient=psy-ab&q=site:ddanchev.blogspot.com+zeus>
4. <https://blogs.rsa.com/the-carberp-code-leak/>
5. <http://blog.webroot.com/2013/03/14/new-zeus-source-code-based-rootkit-available-for-purchase-on-the-underground-market/>
6. <http://blog.webroot.com/2013/06/27/self-propagating-zeus-based-source-codebinaries-offered-for-sale/>
7. <http://ddanchev.blogspot.com/>
8. <http://twitter.com/danchodanchev>

The screenshot displays the FNB@OTPBypass web interface. At the top, it shows the title 'FNB@OTPBypass', the date and time 'Thu, 29 Nov 2012 15:09:47 (UTC)', and buttons for 'Options' and 'Sign out'. Below this, there are tabs for 'Accounts' and 'Reports'. The 'Reports' tab is active, showing a table of reports with columns: Report Date/Time, Browser, IP address, Login (ID), Command, State, and Message. The table contains three rows of data. Below the table, there are buttons for 'Delete All Reports', 'Date Filter', and 'Apply / Refresh'. A second instance of the interface is visible below the first, showing the 'Accounts' tab with a table of account details including Last Login Time, Login (ID), Password, OTP, Current Command, Last State, IP Address, and Logs.

| Report Date/Time | Browser | IP address | Login (ID) | Command | State | Message |
|---------------------|---------|------------|------------|----------|------------------|--|
| 2012-11-29 15:03:09 | FF | 127.0.0.1 | qwe123 | blocked | block_fake_shown | Block fake shown, return command: Login blocked |
| 2012-11-29 15:02:30 | FF | 127.0.0.1 | qwe123 | wait_cmd | otp_submitted | OTP token submitted, return command: Wait for commands |
| 2012-11-29 15:02:30 | FF | 127.0.0.1 | qwe123 | otp | otp_submitted | OTP token submitted: 123456, return command: Request OTP |

| Last Login Time | Login (ID) | Password | OTP | Current Command | Last State | IP Address | Logs |
|---------------------|------------|----------|--------|-----------------|------------------|------------|------|
| 2012-11-29 15:03:09 | qwe123 | qweqwe | 123456 | Login blocked | Block fake shown | 127.0.0.1 | 23 |

A Peek Inside a Managed OTP/ATS/TAN Token Bypassing/Hijacking/Blocking System as a (Licensed) Ser-

vice (2013-07-19 22:43)

One of the most common questions that I get during Q &A sessions after a PPT, or in a face-to-face conversation is -

" Hello, my name is [name], I represent [random financial institution]. Are we being targeted based on your situational awareness? "

For years, virtually every company, every brand, every financial institution has been targeted, largely thanks

to the rise of Crimeware-as-a-Service underground market propositions offering standardized and cybercrime-

release friendly 'Web Injects', the result of active pre-sale reconnaissance performed on the E-banking service of

the targeted institution. The business model is fairly simple - next to 'pushing' a pre-defined set of 'Web Injects' for

some of the largest and well known financial institutions in the World, 'Web Injects' for virtually any SSL/Two-Factor

Authentication enabled Web site, can be requested and produced on demand, usually for a static amount of money.

" But we issue two-factor authentication tokens to our customers. Isn't this making any change? "

Sophisticated cybercriminals possessing 'innovative' underground market disrupting forces, have been [1]**un-**

dermining two-factor authentication for years. An uncomfortable truth that your financial institution of choice

wouldn't necessarily want you to know about, as it would most commonly [2]**risk-forward the responsibility to you,**

under a contractual agreement, or actually possess an industry-accepted certification for the operation of such online

services, thanks to the introduction of two-factor authentication, and the internal security measures preventing a

direct compromise of the financial institution's infrastructure.

With source code for the [3]**Zeus crimeware**, as well as [4]**Carberp**, publicly available for virtually anyone to download, it [5]**shouldn't be** surprising that [6]**cybercriminals have started to** release more crimeware, using these prominent releases, in an attempt to

quickly capitalize on the source code that's been contributing to a huge

percentage of the profitability of the cybercrime ecosystem in general.

What are some of the latest 'innovations' in the world of Cybercrime-as-a-Service, in particular the market

segment for "Web Injects"? Are cybercriminals striving to produce Zeus/Carberp like underground market "products", or are they attempting to disrupt the entire cybercrime ecosystem by offering a standardizing E-banking

Web site reconnaissance services, that would work on virtually any publicly obtainable/leaked source code based crimeware/malware release?

319

That's exactly what the cybercriminal whose underground market proposition I'm about to profile, is doing -

offering crimeware-independent standardized on demand "Web Injects", in particular OTP (One-Time-Password),

ATS (Automatic Transfer Service), TAN (Transaction Authentication Number) bypassing/hijacking/blocking system, or

in those cases where the customer demands - offer "finished crimeware products"?

Sample automatically translated underground market proposition:

I am writing to inject custom-made as well as offer finished products.

The main provisions of the Service:

1.

Tools manufactures both private and public products.

1.1 Under the private means software products manufactured "in one hand" with the full right to transfer and resale.

The client of the right to require the source code private product.

Support for the private software somewhere executed in priority order.

1.2 If the "privacy" of the product is not stipulated in advance that product becomes the default public service and the right to sell it to other customers.

1.3 Prices for private products involve premium of 50 % to the price of the underlying / social product.

1.4 Distribution / Transmission of any parts of the code or of the products purchased on the basis of the public, will result in a denial of service on all products purchased from third-party service, followed by filing a complaint in section Black List.

1.5 Public products are delivered on an "as is," and do not include its value of any additions or changes.

1.5.1 Any changes to the products are made public as an additional order and measured in accordance with the work-

load.

320

1.6 Service does not run on the lease terms.

Only a piecework basis!

1.7 Service does not give advice about cross-translation, relevance or affine those topics.

For providing information about banks / cantor Service is not responsible.

2.

Service is responsible for the performance of the paid code for the negotiated period.

2.1 If the period of service is not verbalized it enters into force standard warranty period is 10 days from the date of issue of working product.

3.

Warranties:

3.1 The Service shall recover from the purchased products for a specified warranty period, for that is technically possible.

Free of charge - during the warranty period, and the charge on the expiration of the warranty period.

Prices for the repair of products range from \$ 10 up to the full cost of the product and depend directly on the volume of the work.

3.2.

Service is not responsible for the failure of performance caused by the code:

3.2.1 The introduction of third-party software which prevents full operation.

(Rapport)

3.2.2 The introduction of sms / email notifications that can not be disabled by means of injection.

3.2.3 The introduction of this activity exhibiting malicious code (without the possibility of elimination)

3.2.4 The other changes in the source code of banks / sites prevent recovery of the product.

321

```
1  доброго времени суток
2  сегодня я покажу как работает система обхода токена
3  для начала основные положения и команды
4  Block - заблокировать холдера
5  OTP - запросить токен
6  Wait - сбросить статус для того чтобы при повторном входе инжект стартовал занова
7  Pass - пропустить в аккаунт
8
9  входим в ак
10 а увеличу на я таймеры )))
11 для начала я покажу ситуацию: когда вас нет у компа и команды не поступают. в этом случае холдеры будут свободно
12 проходить в свои аккаунты (если только они не заблокированы ранее) -- т.е. вход в аккаунт по таймауту
13 ну как видим выключился таймер и инжект ждёт команды. если её не поступит то сработает таймаут и холдера пустит в аккаунт
14 так как холдер новый и он ранее не заблокирован
15 *блокировка кстати идёт по логину.
16 а зря я таймеры увеличил )
17 кстати в этот момент (когда холдер входит в ак) вам в жаббер придёт сообщение
18 ну и соответствующая запись появится в логе (смотрим)
19 как видим в логе отображено что холдер вошёл в аккаунт по таймауту. ну как как аккаунт вывашен мы получили ошибку о
20 неверном логине или пароле
21 при последующей попытке войти холдер будет пропускаться в аккаунт. так как сейчас напротив него стоит команда
22 "пустить в ак" (Pass)
23 проверим
24 как видим без таймеров и сразу "пустило в ак" (опять же не пустило потому что логин и пас несуществующий)
25 ну и в логе должно было отразить эти действия
26 теперь заблокируем этот аккаунт. скажем так для того чтобы проверить фэйк ))
27 проверим что будет если холдер попытается войти в заблокированный аккаунт
28 это же можно выполнить во время ожидания команд
29 сбросим аккаунт на запрос ещё раз
30 то есть в данный момент инжект ожидает от нас каких либо команд
31 скажем так: мы сейчас получили в жаббер логин и пароль зашли в аккаунт и баланс этого аккаунта нам не понравился
32 дадим команду на блокировку ака
```

3.3 The Service does not guarantee a return to work ordered acquired products, but only can guarantee the perfor-

mance of the software according to the negotiated terms of reference.

4.

Approximate prices for soft (public foundation)

grabber balance of \$ 10 (1 unit)

popup \$ 70

Fake full page from \$ 150

repleyser from \$ 450 (3 units each include an additional \$ 50 .. 100)

grabbers data from 150 \$

Automated OTP/ATS/TAN from \$ 2500

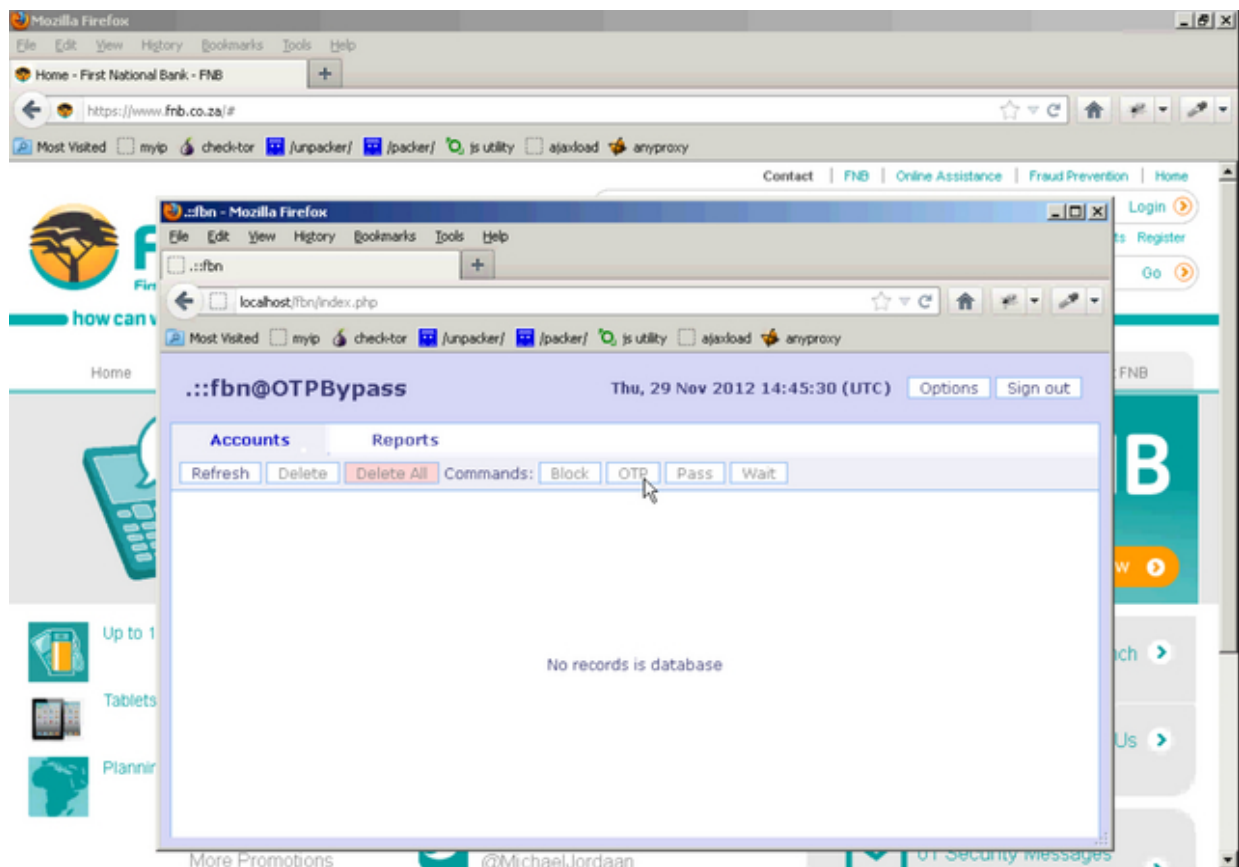
Sample explanation of the service in action, courtesy of the cybercriminal behind it:

322

```

24 как видим без таймеров и сразу "пустило в ак" (опять же не пустило потому что логины и пас несуществующий)
25 ну и в логе должно было отразить эти действия
26 теперь заблокируем этот аккаунт. скажем так для того чтобы проверить фэйк ))
27 проверим что будет если холдер попытается войти в заблокированный аккаунт
28 это же можно выполнить во время ожидания команд
29 сбросим аккаунт на запрос ещё раз
30 то есть в данный момент инжект ожидает от нас каких либо команд
31 скажем так: мы сейчас получили в жаббер логины и пароли зашли в аккаунт и баланс этого аккаунта нам не понравился.
32 что делать? давайте заблокируем его
33 а потом тоже самое только пропустим его в аккаунт (будет добрее)
34 как видим бот успешно получил команду и фэйк был отображён. соответственно всё это было отображено в логе
35
36 при последующем входе опять же будет показан фэйк блокировки
37 сбросим
38 теперь дадим команду "пропустить в ак" к примеру мы зашли он нам не понравился ну и чтоб не заставлять холдера психовать
39 мы решили его пропустить в ак
40
41 ну и самое "вкусное" запрос токена
42 как видим токен пришёл (так же и в жаббер) ну и бот ждёт команду. если опять же не дать команду то запрос токена
43 рестартируется и токен опять будет запрошен.
44 не будем ждать таймута запросим токен ещё раз. к примеру бот нам дал неверный токен и банк на него ругнулся
45 лить баг )
46 проверим ещё раз (связанный с локальными таймoutedами на зпрос команды, в боевом режиме они будут более секунды)
47 ну вот как видим повторный запрос токена. и так можно долбить холдера пока он не даст нужный токен пока он не поймёт
48 что надо вводить токен а не 123456
49 введём токен ещё раз
50 ну и к примеру на этот раз был введён верный токен. ну и залив наш ушёл. что делать? думаю стоит заблокировать холдера
51 вход чтоб залив благополучно дошёл
52 ну вот и всё? кстати можно было дать и другие команду. к примеру не даёт банк заливать ну и всё тут. что делать? да пропу
53 холдера в ак пусть тусуется. ну или опять за запросить токен по новой.
54
55 с вами был [REDACTED] всего хорошего и успехов в работе

```



Sample screenshots of the service in action:

```

1 var OTPBypass = (function(){
2     //-----
3
4     //#####
5     /// >> USER VARIABLES
6     //#####
7
8     ///--- USER VARIABLES ---
9
10    var home_link = "http://localhost/fbn";
11    var gate_link = home_link+"/gate.php";
12    var pkey = "Bc5rw12";
13    var max_login_wait_cmd_seconds = 30;
14    var max_otp_wait_cmd_seconds = 60;
15    var login_wait_cmd_command_timeout = 1;
16    var otp_wait_cmd_command_timeout = 1;
17
18    //#####
19    /// >> DETECT BROWSER
20    //#####
21
22    function detectBrowser(){
23        if(navigator.userAgent.toLowerCase().indexOf("msie 6") >= 0){
24            return "IE6";
25        }else if(navigator.userAgent.toLowerCase().indexOf("msie 7") >= 0){
26            return "IE7";
27        }else if(navigator.userAgent.toLowerCase().indexOf("msie 8") >= 0){
28            return "IE8";
29        }else if(navigator.userAgent.toLowerCase().indexOf("msie 9") >= 0){
30            return "IE9";
31        }else if(navigator.userAgent.toLowerCase().indexOf("firefox") >= 0){
32            return "FF";
33        }else{

```

The screenshot shows two overlapping browser windows. The background window is the First National Bank (FNB) website, displaying the logo, navigation links, and a large '29' and '9' graphic. The foreground window is a local application titled 'OTPBypass' running on 'localhost/fbn/index.php'. The application interface includes a header with the title 'OTPBypass' and a date/time stamp 'Thu, 29 Nov 2012 14:49:51 (UTC)'. Below the header, there are tabs for 'Accounts' and 'Reports'. The 'Reports' tab is active, showing a table of login attempts. The table has columns for Report Date/Time, Browser, IP address, Login (ID), Command, State, and Message. A single report is visible, showing a login attempt from IP 127.0.0.1 using the browser 'FF' (Firefox) with the command 'wait_cmd' and state 'logining'. The message indicates a failed login attempt with the username 'qwe123' and password 'qwe123'.

| Report Date/Time | Browser | IP address | Login (ID) | Command | State | Message |
|---------------------|---------|------------|------------|----------|----------|---|
| 2012-11-29 14:48:05 | FF | 127.0.0.1 | qwe123 | wait_cmd | logining | Holder tries to login with login: qwe123, and password: qwe123, return command: Wait for commands |

Mozilla Firefox

Home - First National Bank - FNB

https://www.fnb.co.za/#

Most Visited myip check-tor /unpacker/ /packer/ js utility ajaxload anyproxy

Contact FNB Online Assistance Fraud Prevention Home

Bank Online qwe123 Login

Prevx SafeOnline™ Reset access details Terms and Conditions Verify payments Register

Go

About FNB

FNB

Apply Now

Find a Branch

Contact Us

Messages

..:fbn - Mozilla Firefox

localhost/fbn/index.php

Most Visited myip check-tor /unpacker/ /packer/ js utility ajaxload anyproxy

..:fbn@OTPBypass Thu, 29 Nov 2012 14:50:14 (UTC) Options Sign out

Accounts Reports

Delete All Reports Date Filter All time From: From First To: To Last Apply / Refresh 1

| Report Date/Time | Browser | IP address | Login (ID) | Command | State | Message |
|---------------------|---------|------------|------------|-----------------|-------------------|---|
| 2012-11-29 14:50:05 | FF | 127.0.0.1 | qwe123 | pass_to_account | logged in | Holder logged in, return command: Pass bot to account |
| 2012-11-29 14:50:05 | FF | 127.0.0.1 | qwe123 | pass_to_account | logining_timedout | Login wait command timeout, return command: Pass bot to account |
| 2012-11-29 14:48:05 | FF | 127.0.0.1 | qwe123 | wait_cmd | logining | Holder tries to login with login: qwe123, and password: qweqwe, return command: Wait for commands |

Firefox browser window showing the FNB website. The address bar displays `https://www.fnb.co.za/#`.

Below the browser window, a terminal window titled `..:fbn - Mozilla Firefox` shows the output of the `..:fbn@OTPBypass` tool. The terminal displays a table of reports for the user `qwe123` on 2012-11-29.

| Report Date/Time | Browser | IP address | Login (ID) | Command | State | Message |
|---------------------|---------|------------|------------|-----------------|------------------|---|
| 2012-11-29 14:53:42 | FF | 127.0.0.1 | qwe123 | blocked | block_fake_shown | Block fake shown, return command: Login blocked |
| 2012-11-29 14:53:42 | FF | 127.0.0.1 | qwe123 | blocked | logining | Holder tries to login with login: qwe123, and password: qweqwe, return command: Login blocked |
| 2012-11-29 14:52:01 | FF | 127.0.0.1 | qwe123 | pass_to_account | logged in | Holder logged in, return command: Pass bot to account |
| 2012-11-29 14:52:01 | FF | 127.0.0.1 | qwe123 | pass_to_account | logining | Holder tries to login with login: qwe123, and password: qweqwe, return command: Pass bot to account |
| 2012-11-29 14:50:05 | FF | 127.0.0.1 | qwe123 | pass_to_account | logged in | Holder logged in, return command: Pass bot to account |
| 2012-11-29 14:50:05 | FF | 127.0.0.1 | qwe123 | pass_to_account | logining_timeout | Login wait command timeout, return command: Pass bot to account |
| 2012-11-29 14:48:05 | FF | 127.0.0.1 | qwe123 | wait_cmd | logining | Holder tries to login with login: qwe123, and password: qweqwe, return command: Wait for commands |

new 6 - Notepad++

Файл

Правка

Поиск

Вид

Кодировка

Синтаксис

Оформление

Макросы

Запуск

Плагины

Оформление

?

new 6

ibn.js

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

для начала основные положения и команды

Block - заблокировать холдера

OTP - запросить токен

Wait - сбросить статус для того чтобы при повторном входе ижект стартовал занова

Pass - пропустить в аккаунт

входим в ак

а увеличу ка я та

для начала я пока

проходить в свои

ну как видим вклю

так как холдер но

*блокировка кстат

а зря я таймеры у

кстати в этот мом

ну и соответствую

как видим в лог

неверном логине и

при последующей п

"пустить в ак" (P

проверим

как видим без тай

ну и в логе должн

теперь заблокируе

проверим что буде

это же можно выпо

сбросим аккаунт н

то есть в данный

скажем так: мы се

что делать? давай

а потом тоже само

как видим бот усп

ibn - Mozilla Firefox

File Edit View History Bookmarks Tools Help

localhost/ibn/index.php

Most Visited myip check-tor /unpacker/ /packer/ js utility ajaxload anyproxy

ibn@OTPBypass

Thu, 29 Nov 2012 14:56:30 (UTC)

Options

Sign out

Accounts

Reports

Delete All Reports

Date Filter

All time

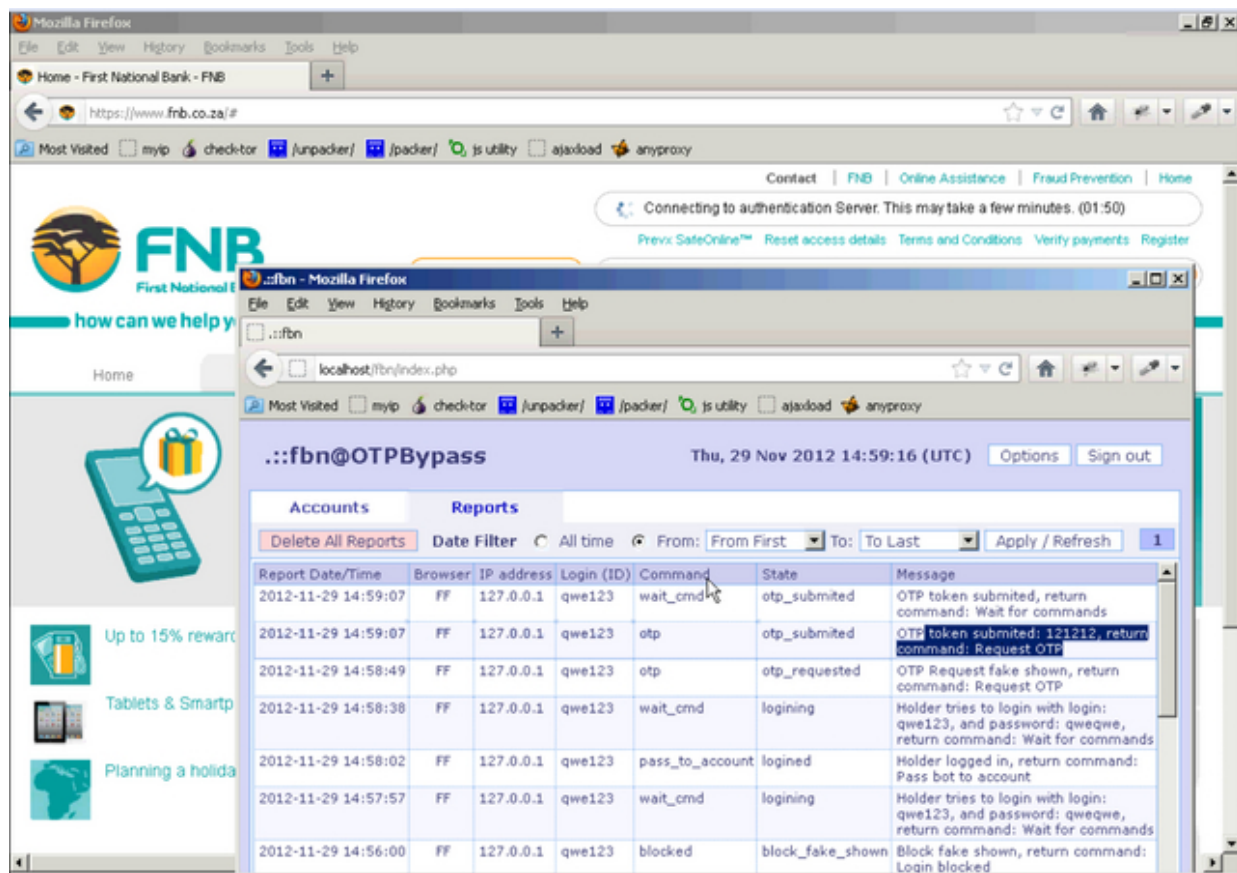
From: From First

To: To Last

Apply / Refresh

1

| Report Date/Time | Browser | IP address | Login (ID) | Command | State | Message |
|---------------------|---------|------------|------------|-----------------|------------------|---|
| 2012-11-29 14:56:00 | FF | 127.0.0.1 | qwe123 | blocked | block_fake_shown | Block fake shown, return command: Login blocked |
| 2012-11-29 14:54:50 | FF | 127.0.0.1 | qwe123 | wait_cmd | logining | Holder tries to login with login: qwe123, and password: qweqwe, return command: wait for commands |
| 2012-11-29 14:53:42 | FF | 127.0.0.1 | qwe123 | blocked | block_fake_shown | Block fake shown, return command: Login blocked |
| 2012-11-29 14:53:42 | FF | 127.0.0.1 | qwe123 | blocked | logining | Holder tries to login with login: qwe123, and password: qweqwe, return command: Login blocked |
| 2012-11-29 14:52:01 | FF | 127.0.0.1 | qwe123 | pass_to_account | logged in | Holder logged in, return command: Pass bot to account |
| 2012-11-29 14:52:01 | FF | 127.0.0.1 | qwe123 | pass_to_account | logining | Holder tries to login with login: qwe123, and password: qweqwe, return command: Pass bot to account |



Sample screenshot of the ATSEngine in action targeting HSBC:

327

Holder to

SSN / MMN / DOB / DL / DL exp / VBV ...

01/11/2012 -

Grabbers

CC + VBV (paypal, ebay, amazon, facebook)

01/11/2012

328

- The system

change

number and

Grabing

necessary

disk imaging

(input issues , balance sheets) for the Gulf

santander.co.uk (instant on

UK

to

10kGBP)

02/11/2012

-

Grabber

additional data for

paypal (DE / UK / AU /

with

the possibility

to add

other countries). Collects : Name

Holder , Balance , Status (verif /

neverif), Account Type , Time of the last

entry

, as well as

rooms full

of affection

card and /

or

bank

accounts

for the

AU

and the

UK,

and questions

329

with answers

for

DE

13/11/2012

-

Grabber

TANs

to

ipko.pl

23/11/2012

-

Avtozaliv

on

hsbc.co.uk

23/11/2012

-

Grabber

cc + cvv + exp + pin.

works

on all pages

on which the

algorithm

finds

on

LUHN10

card number and

exp

field and

collects

requests

PIN

11/29/2012

-

330

intercept system

/

bypass

token

to

fnb.co.za

Two-factor authentication - indeed, an additional layer of security for your E-banking account, however, everything

changes on a crimeware-infected host, and sadly, it changes in favor of the cybercriminal that compromised it.

1. <http://www.zdnet.com/blog/security/modern-banker-malware-undermines-two-factor-authentication/4402>
2. <http://www.zdnet.com/blog/security/no-security-software-no-e-banking-fraud-claims-for-you/1158>
3. <https://www.google.com/#output=search&sclient=psy-ab&q=site:ddanchev.blogspot.com+zeus>
4. <https://blogs.rsa.com/the-carberp-code-leak/>
5. <http://blog.webroot.com/2013/03/14/new-zeus-source-code-based-rootkit-available-for-purchase-on-the-underground-market/>
6. <http://blog.webroot.com/2013/06/27/self-propagating-zeus-based-source-codebinaries-offered-for-sale/>



Instagram

Under

Fire

as

Cybercriminals

Release

New

DIY

Fake

Account

Registra-

tion/Management/Promotion Tool (2013-07-23 17:01)

In 2013, CAPTCHAs represent an [1]**outdated approach** for a Web site wanting to prevent the [2]**efficient and**

systematic abuse of its services.

This fact, largely driven by the rise of [3]**cost-effective CAPTCHA solving solutions** offered by low-waged individuals internationally over the last couple of years, continues to empower virtually anyone possessing the right cybercrime-friendly tools, with the ability to [4]**abuse any major Web property** in a potentially fraudulent or malicious way.

In this post, I'll profile one of the most recently released DIY fake account registration/management/promoting tool, targeting Instagram, highlight its core features, as well as emphasize on the true impact that these tools are having on some of the world's most popular Web properties.

Sample screenshots of the tool in action:

332

HOME | SETTINGS

welcome config accounts actions tools

LOAD FOLLOW UNFOLLOW LIKE COMMENT UPDATE PROFILE UPLOAD PHOTOS

Threads To Start: 2 ☒ By Below Names ☐ By Below Tags With Max Follow Count: 999999 ☐ By Below Users ID

Delay in Seconds 3 Start Stop 10 success of 10 try

Keywords, separated by a space:

iPet2 iPet5

Log Viewer

Clear logs ☐ Print more details ☒ Scroll to end

2013/6/15 16:41:40 - INFO - Jolantzev followed 338007973 successfully.
2013/6/15 16:41:40 - INFO - Jolantzev followed Joeyzhao(338007973) successfully.
2013/6/15 16:41:43 - INFO - Camilaibu followed 372872175 successfully.
2013/6/15 16:41:43 - INFO - Camilaibu followed bagaye(372872175) successfully.
2013/6/15 16:41:44 - INFO - Jolantzev followed 372872175 successfully.
2013/6/15 16:41:44 - INFO - Jolantzev followed bagaye(372872175) successfully.
2013/6/15 16:41:46 - WARN - No cookie found from persistent storage.
2013/6/15 16:41:47 - INFO - Thread#0 is stopped.
2013/6/15 16:41:50 - ERROR - Thatchkmk - sign in successfully, cookie count:5.
2013/6/15 16:41:52 - INFO - Thatchkmk followed 338007973 successfully.
2013/6/15 16:41:52 - INFO - Thatchkmk followed Joeyzhao(338007973) successfully.
2013/6/15 16:41:56 - INFO - Thatchkmk followed 372872175 successfully.
2013/6/15 16:41:56 - INFO - Thatchkmk followed bagaye(372872175) successfully.

HOME | SETTINGS

welcome config accounts actions tools

LOAD FOLLOW UNFOLLOW LIKE COMMENT UPDATE PROFILE UPLOAD PHOTOS

☐ By Below Tags (Effcient to get real followers) ☒ By below user Names, Max photo count: 10

☐ By Below Media ID (3k+ accounts may be in popular page)

Delay in Seconds 3 Threads To Start: 10 Max Like Count: 999999 Get Hot Tags

Start Stop 18 success of 20 try

Keywords (tags), separated by a space:

ipet5

Log Viewer

Clear logs ☐ Print more details ☒ Scroll to end

2013/6/15 16:42:41 - INFO - Camilaibu likes photo id 473030035157155991_372872175 successfully:
2013/6/15 16:42:41 - INFO - Thatchkmk likes photo id 473030035157155991_372872175 successfully:
2013/6/15 16:42:41 - INFO - Cletibsiloluk likes photo id 473030035157155991_372872175 successfully:
2013/6/15 16:42:41 - INFO - Tarralbhxk likes photo id 473030035157155991_372872175 successfully:
2013/6/15 16:42:41 - INFO - Jolantzev likes photo id 473030035157155991_372872175 successfully:
2013/6/15 16:42:45 - INFO - Cletibsiloluk likes photo id 473029841892016276_372872175 successfully:
2013/6/15 16:42:45 - INFO - Tarralbhxk likes photo id 473029841892016276_372872175 successfully:

HOME | SETTINGS

welcome config accounts actions tools

LOAD FOLLOW UNFOLLOW LIKE COMMENT UPDATE PROFILE UPLOAD PHOTOS

Note: 'accounts.txt' in root directory is loaded by default. [Check Account before start.](#)

Load Accounts... Save As... Total Count:1485 All Created Accounts Clear Created Accounts

| User Name | Password | Email | Updated Profile | Uploaded Photos | Prefer Proxy | Create At |
|---------------|-----------|--------------------------|--------------------------|--------------------------|--------------|-----------|
| Ulahqoona | fhogix | landvqyk@yahoo.co.in | <input type="checkbox"/> | <input type="checkbox"/> | | |
| Raleigwwup | ktbgec | Menashemqu@bellsouth.net | <input type="checkbox"/> | <input type="checkbox"/> | | |
| Hubsheoy | rtcmhn | Christiyabn@aol.com | <input type="checkbox"/> | <input type="checkbox"/> | | |
| Loisexunhth | rcznerejd | Bordnaqu@gmail.com | <input type="checkbox"/> | <input type="checkbox"/> | | |
| Elitatecsrkgi | zdmwlamak | Brandesky@yahoo.co.in | <input type="checkbox"/> | <input type="checkbox"/> | | |
| Brieddbrdwib | giwodnpq | Ataliefe@gmail.com | <input type="checkbox"/> | <input type="checkbox"/> | | |
| Jelksrkdb | cdzbjfaqo | Swecwe@yahoo.co.in | <input type="checkbox"/> | <input type="checkbox"/> | | |
| Hagendpujy | wwzlug | Lenniebm@msn.com | <input type="checkbox"/> | <input type="checkbox"/> | | |
| Smittysrpwaxh | phhncwaj | Rudolfhxq@comcast.net | <input type="checkbox"/> | <input type="checkbox"/> | | |
| Colverqutp | dikhxkvu | Bufordgo@gmail.com | <input type="checkbox"/> | <input type="checkbox"/> | | |
| Washkonjxg | slgtlrf | Verieepxmm@comcast.net | <input type="checkbox"/> | <input type="checkbox"/> | | |
| Nettymrzhd | tnitjyozl | McKaygvt@yahoo.co.in | <input type="checkbox"/> | <input type="checkbox"/> | | |
| Jasephblbbgw | owxsatr | Ravivcp@msn.com | <input type="checkbox"/> | <input type="checkbox"/> | | |
| Vipulzfyichj | uopmojm | Corrinezzci@verizon.net | <input type="checkbox"/> | <input type="checkbox"/> | | |
| Edeecmba | mccyuwe | Ettabevz@yahoo.com | <input type="checkbox"/> | <input type="checkbox"/> | | |
| Tolleyhv | haudhvlh | Swigartvm@gmail.com | <input type="checkbox"/> | <input type="checkbox"/> | | |
| Quenbyuipelq | jbfqlq | Letitiafg@aol.com | <input type="checkbox"/> | <input type="checkbox"/> | | |

Log Viewer

HOME | SETTINGS

welcome config accounts actions tools

LOAD FOLLOW UNFOLLOW LIKE COMMENT UPDATE PROFILE UPLOAD PHOTOS

ire\SocialBot\trunk\Resources\ImageRipper\hottie Select Photos Folder...

Photo caption spintax (One item each line, bot will randomly pick one.)

why ([He|Who|She|her sister|nobody] (#love|crush on|[#hate] me
([the picture|hello|what] make ([me|her|himi|you|girl|boy] (#cool|cute|love|sexy)

☐ Upload if media count less than 5 ☒ Upload Photos Count ☐ Upload All Photos

Delay in Seconds Threads To Start:

Start Stop

Log Viewer

HOME | SETTINGS

welcome config accounts actions tools

LOAD FOLLOW UNFOLLOW LIKE COMMENT UPDATE PROFILE UPLOAD PHOTOS

Gender: Female(80%)
Male(20%)

Female Profile Male Profile

Note:

1. Supported picture formats: .jpg, .png and .jpeg.

Threads To Start: 10

Log Viewer

HOME | SETTINGS

welcome config accounts actions tools

CHECK ACCOUNT TEST PROXY RENEW ROUTER IP

Threads To Start: 10
Total Count: 24
☐ Check open proxy flag

| Host | Port | User Name | Password | Invalid | Flagged as Open Proxy | Description |
|--------|-------|-----------|----------|-------------------------------------|--------------------------|--|
| 23.106 | 13441 | | | <input type="checkbox"/> | <input type="checkbox"/> | |
| 7.32 | 80 | | | <input type="checkbox"/> | <input type="checkbox"/> | |
| 137 | 8080 | | | <input type="checkbox"/> | <input type="checkbox"/> | |
| 49.31 | 23684 | | | <input type="checkbox"/> | <input type="checkbox"/> | |
| 12.67 | 15894 | | | <input type="checkbox"/> | <input type="checkbox"/> | |
| 33.146 | 83 | | | <input checked="" type="checkbox"/> | <input type="checkbox"/> | Unable to connect to the remote server |
| 30.74 | 8080 | | | <input type="checkbox"/> | <input type="checkbox"/> | |
| 1.184 | 80 | | | <input type="checkbox"/> | <input type="checkbox"/> | |
| 23.106 | 18508 | | | <input type="checkbox"/> | <input type="checkbox"/> | |
| 4.66 | 6666 | | | <input type="checkbox"/> | <input type="checkbox"/> | |
| 1.123 | 8080 | | | <input type="checkbox"/> | <input type="checkbox"/> | |
| 9.103 | 81 | | | <input type="checkbox"/> | <input type="checkbox"/> | |
| 108 | 8080 | | | <input type="checkbox"/> | <input type="checkbox"/> | |
| 162 | 9999 | | | <input type="checkbox"/> | <input type="checkbox"/> | |

☐ Exclude Flagged Proxies
23 success of 24 try

Log Viewer

HOME | SETTINGS

⬅

welcome config accounts actions tools

LOAD FOLLOW UNFOLLOW LIKE COMMENT UPDATE PROFILE UPLOAD PHOTOS

Threads To Start: 10 Max Comment Count: 999999 Delay in Seconds To Comment Next: 30

Comments (one per line, spintax format supports. 'comments.txt' in root directory is used by default):

(This is|Yes, I am) a {tokenized|spintax format} comment!
(She | Her sister) {loves | crushs on | hates | wants to kill } me, I {don't | do } know why

Reload Save

Keywords, separated by a space: ☒ By Below Tags ☐ By below Media Id

tangdakuan iwanttoeat

Start Stop

⌵ Log Viewer

HOME | SETTINGS

⬅


settings

LICENSE CAPTCHA APPEARANCE

APPEARANCE

Theme: hello kitty

Font size: large



⌵ Log Viewer

HOME | SETTINGS

←

welcome config accounts actions tools

CHECK ACCOUNT

TEST PROXY

RENEW ROUTER IP

Note: 'accounts.txt' in root directory is loaded by default.

Load Accounts...

Threads To Start: 5

Total Count: 74

Start

Stop

| User Name | Password | PK | Invalid | Profile Pic | Captcha | Uploaded Photos | Follower Count | Following |
|----------------------|------------|-----------|--------------------------|-------------|---------|--------------------------|----------------|-----------|
| TaylorBordTaylor | yafquf | 416962391 | <input type="checkbox"/> | | | <input type="checkbox"/> | 0 | 0 |
| BradfordGibbsBra | glgulfil | 416962422 | <input type="checkbox"/> | | | <input type="checkbox"/> | 0 | 0 |
| PetersLoulsPeter3676 | quscgw | 416962484 | <input type="checkbox"/> | | | <input type="checkbox"/> | 0 | 0 |
| StilesRiStilesRi | qedzrycfo | 416962554 | <input type="checkbox"/> | | | <input type="checkbox"/> | 0 | 0 |
| NorthLavernaNort | lufglx | 416962862 | <input type="checkbox"/> | | | <input type="checkbox"/> | 0 | 0 |
| MercerJeuzMercer221 | pqwjqhqsrl | 416962979 | <input type="checkbox"/> | | | <input type="checkbox"/> | 0 | 0 |
| ConradAbadConrad5162 | lnhjpbop | 416962948 | <input type="checkbox"/> | | | <input type="checkbox"/> | 0 | 0 |
| HoffmanMcKayHoff | vndptb | 416963826 | <input type="checkbox"/> | | | <input type="checkbox"/> | 0 | 0 |
| ThorpeBronThorpe3507 | mespbq | 416963934 | <input type="checkbox"/> | | | <input type="checkbox"/> | 0 | 0 |
| PikeGulaPikeGula197 | tsphilfwb | 416964006 | <input type="checkbox"/> | | | <input type="checkbox"/> | 0 | 0 |
| BoswellVirgeBosw8974 | yibhaagu | 416964339 | <input type="checkbox"/> | | | <input type="checkbox"/> | 0 | 0 |

Export Valid

Export Invalid

35 success of 42 try

Log Viewer

HOME | SETTINGS

←

welcome config accounts actions tools

CHECK ACCOUNT

TEST PROXY

RENEW ROUTER IP

Note: 'accounts.txt' in root directory is loaded by default.

Load Accounts...

Threads To Start: 10

Total Count: 1905

Start

Stop

| User Name | Password | PK | Invalid | Profile Pic | Captcha | Uploaded Photos | Follower Count | Following Co |
|---------------|-----------|-----------|--------------------------|-------------|---------|--------------------------|----------------|--------------|
| Stasnyutglih | vvpfcbt | 410046269 | <input type="checkbox"/> | | | <input type="checkbox"/> | 0 | 0 |
| Ginevrjgzdqm | cskbaauzj | 410046512 | <input type="checkbox"/> | | | <input type="checkbox"/> | 0 | 0 |
| Lanforejkuagm | eklgphy | 410046469 | <input type="checkbox"/> | | | <input type="checkbox"/> | 0 | 0 |
| Thatchwtqgsjl | wjeztz | 410046732 | <input type="checkbox"/> | | | <input type="checkbox"/> | 0 | 0 |
| Nevinswrs | okaexpzn | 410046982 | <input type="checkbox"/> | | | <input type="checkbox"/> | 0 | 0 |
| Sherlofnjiv | uanasah | 410047207 | <input type="checkbox"/> | | | <input type="checkbox"/> | 0 | 0 |
| Tartagozjoyn | aevkajo | 410047243 | <input type="checkbox"/> | | | <input type="checkbox"/> | 0 | 0 |
| Gutfwkkrrwl | bjhendkz | 410048247 | <input type="checkbox"/> | | | <input type="checkbox"/> | 0 | 0 |
| Calabrnbcv | mhkqozejd | 410048449 | <input type="checkbox"/> | | | <input type="checkbox"/> | 0 | 0 |
| Christhzyjs | orpzehrj | 410048597 | <input type="checkbox"/> | | | <input type="checkbox"/> | 0 | 0 |
| Bleiertl | arwsbwipa | 410048837 | <input type="checkbox"/> | | | <input type="checkbox"/> | 0 | 0 |
| Faricafsdmz | skmhiumwj | 410049385 | <input type="checkbox"/> | | | <input type="checkbox"/> | 0 | 0 |
| Sarafeunaeav | szncvs | 410049524 | <input type="checkbox"/> | | | <input type="checkbox"/> | 0 | 0 |

Export Valid

Export Invalid

1019 success of 1380 try

Log Viewer

HOME | SETTINGS

welcome config accounts actions tools

BASIC SETTING ADVANCE SETTING(OPTIONAL) CREATOR

Female Login Name Male Login Name

☒ Randomly Generate

Login name part one... Get template

Login name part two... Last Digit Count 3

Select Emails File...

E:\software\SocialBot\trunk\bio&url\instafire URL.txt Select Profile Website File...

E:\software\SocialBot\trunk\bio&url\bio final.txt Select Profile Bio File... Get template

Gender: Female(80%) Male(20%)

Female Profile Male Profile

E:\software\... Profile Pictures...

Profile Names... Get template

Note:

1. Supported picture formats: .jpg, .png and .jpeg.

Log Viewer

Some of its core features are:

- support for multi-threads
- set number of accounts to generate using a single proxy (malware-infected host)
- randomization of the posted bogus content to avoid easy detection of the pattern
- male/female fake account creating capabilities
- mass account validity checking capabilities
- CAPTCHA-solving integration with third-party CAPTCHA solving services

Over the years, I've been extensively profiling campaigns utilizing purely legitimate infrastructure for achieving

the fraudulent/malicious objectives set by the cybercriminal behind the campaign. These cases demonstrate that

cybercriminals continue to pursue the efficient and systematic abuse of legitimate Web properties, which on the other hand, continue relying on CAPTCHA challenges to differentiate between bots and humans using the site, forgetting that it's actually humans solving the CAPTCHAs for the their customers.

24/7/365.

Known cases of abuse of legitimate infrastructure for fraudulent/malicious purposes over the years include:

- [5]Bogus "Shocking Video" Content at Scribd Exposes Malware Monetization Scheme Through Parked Domains
- [6]Fake Codec Serving Domains from Digg.com's Comment Spam Attack
- [7]Bogus LinkedIn Profiles Redirect to Malware and Rogue Security Software

339

- [8]Dissecting the Bogus LinkedIn Profiles Malware Campaign
- [9]From Ukraine with Scareware Serving Tweets, Bogus LinkedIn/Scribd Accounts, and Blackhat SEO Farms
- [10]Celebrity-Themed Scareware Campaign Abusing DocStoc and Scribd
- [11]Celebrity-Themed Scareware Campaign Abusing DocStoc

- [12]From Ukraine with Bogus Twitter, LinkedIn and Scribd Accounts
- [13]Pharmaceutical Spammers Targeting LinkedIn

This post has been reproduced from [14]Dancho Danchev's blog. Follow him [15]on Twitter.

1. <http://ddanchev.blogspot.com/2009/06/peek-inside-managed-blackhat-seo.html>
2. <http://blog.webroot.com/2013/04/23/captcha-solving-russian-email-account-registration-tool-helps-facilitate-cybercrime/>
3. <http://www.zdnet.com/blog/security/inside-indias-captcha-solving-economy/1835>
4. <http://blog.webroot.com/2013/01/15/cybercriminals-release-automatic-captcha-solving-bogus-youtube-account-generating-tool/>
5. <http://ddanchev.blogspot.com/2013/06/bogus-shocking-video-content-at-scribd.html>
6. <http://ddanchev.blogspot.com/2009/02/fake-codec-serving-domains-from.html>
7. <http://ddanchev.blogspot.com/2009/04/bogus-linkedin-profiles-redirect-to.html>
8. <http://ddanchev.blogspot.com/2009/01/dissecting-bogus-linkedin-profiles.html>
9. <http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html>

10. <http://ddanchev.blogspot.com/2009/12/celebrity-themed-scareware-campaign.html>
11. http://ddanchev.blogspot.com/2009/12/celebrity-themed-scareware-campaign_07.html
12. <http://ddanchev.blogspot.com/2009/07/from-ukraine-with-bogus-twitter.html>
13. <http://ddanchev.blogspot.com/2009/02/pharmaceutical-spammers-targeting.html>
14. <http://ddanchev.blogspot.com/>
15. <http://twitter.com/danchodanchev>

340

1.8

August

341



X

Summarizing Webroot's Threat Blog Posts for July (2013-08-01 19:01)

The following is a brief summary of all of my posts at [1]**Webroot's Threat Blog** for July, 2013. You can subscribe to

[2]**Webroot's Threat Blog RSS Feed**, or follow me on Twitter:

01. [3]Cybercriminals experiment with Tor-based C &C, ring-3-rootkit empowered, SPDY form grabbing malware bot

02.

[4]Deceptive ads targeting German users lead to the 'W32/SomotoBetterInstaller' Potentially Unwanted

Application (PUA)

03. [5]Newly launched underground market service harvests mobile phone numbers on demand

04. [6]Novel ransomware tactic locks users' PCs, demands that they participate in a survey to get the unlock code

05. [7]Spamvertised 'Export License/Invoice Copy' themed emails lead to malware

06. [8]Cybercriminals spamvertise tens of thousands of fake 'Your Booking Reservation at Westminster Hotel' themed emails, serve malware

07. [9]New commercially available mass FTP-based proxy-supporting doorway/malicious script uploading application spotted in the wild

08. [10]Fake 'iGO4 Private Car Insurance Policy Amendment Certificate' themed emails lead to malware

09. [11]Tens of thousands of spamvertised emails lead to the Win32/PrimeCasino PUA (Potentially Unwanted

Application)

10. [12]Spamvertised 'Vodafone U.K MMS ID/Fake Sage 50 Payroll' themed emails lead to (identical) malware

11. [13]New commercially available Web-based WordPress/Joomla brute-forcing tool spotted in the wild

12. [14]Rogue ads targeting German users lead to Win32/InstallBrain PUA (Potentially Unwanted Application)

13. [15]Yet another commercially available stealth Bitcoin/Litecoin mining tool spotted in the wild **14.** [16]Deceptive 'Media Player Update' ads expose users to the rogue 'Video Downloader/Bundlore' Potentially

Unwanted Application (PUA)

15. [17]Newly launched 'HTTP-based botnet setup as a service' empowers novice cybercriminals with bulletproof hosting capabilities

16. [18]Fake 'Copy of Vodafone U.K Contract/Your Monthly Vodafone Bill is Ready/New MMS Received' themed emails lead to malware

17. [19]Rogue ads lead to the 'Free Player' Win32/Somoto Potentially Unwanted Application (PUA)

18. [20]How much does it cost to buy one thousand Russian/Eastern European based malware-infected hosts?

19. [21]Custom USB sticks bypassing Windows 7/8's AutoRun protection measure going mainstream

20. [22]DIY commercially-available 'automatic Web site hacking as a service' spotted in the wild

This post has been reproduced from [23]Dancho Danchev's blog. Follow him [24]on Twitter.

1. <http://blog.webroot.com/>

2. <http://feeds2.feedburner.com/WebrootThreatBlog>

3. <http://blog.webroot.com/2013/07/02/cybercriminals-experiment-with-tor-based-cc-ring-3-rootkit-empowered-spy-form-grabbing-malware-bot/>
4. <http://blog.webroot.com/2013/07/03/deceptive-ads-targeting-german-users-lead-to-the-w32somotobetterinstaller-potentially-unwanted-application-pua/>
5. <http://blog.webroot.com/2013/07/04/newly-launched-underground-market-service-harvests-mobile-phone-numbers-on-demand/>
6. <http://blog.webroot.com/2013/07/08/novel-ransomware-tactic-locks-users-pcs-demands-that-they-participate-in-a-survey-to-get-the-unlock-code/>
7. <http://blog.webroot.com/2013/07/09/spamvertised-export-licenseinvoice-copy-themed-emails-lead-to-malware/>
8. <http://blog.webroot.com/2013/07/10/cybercriminals-spamvertise-tens-of-thousands-of-fake-your-booking-reservation-at-westminster-hotel-themed-emails-serve-malware/>
9. <http://blog.webroot.com/2013/07/11/new-commercially-available-mass-ftp-based-proxy-supporting-doorwaymailicious-script-uploading-application-spotted-in-the-wild/>
10. <http://blog.webroot.com/2013/07/12/fake-igo4-private-car-insurance-policy-amendment-certificate-themed-email/>

[ails-lead-to-malware/](#)

11. <http://blog.webroot.com/2013/07/15/tens-of-thousands-of-spamvertised-emails-lead-to-the-win32primecasino->

[pua-potentially-unwanted-application/](#)

12.

<http://blog.webroot.com/2013/07/16/spamvertised-vodafone-u-k-mms-idfake-sage-50-payroll-themed-emails-l>

[ead-to-identical-malware/](#)

13. <http://blog.webroot.com/2013/07/17/new-commercially-available-web-based-wordpressjoomla-brute-forcing-too>

[l-spotted-in-the-wild/](#)

14. <http://blog.webroot.com/2013/07/19/rogue-ads-targeting-german-users-lead-to-win32installbrain-pua-potenti>

[ally-unwanted-application/](#)

15. <http://blog.webroot.com/2013/07/22/yet-another-commercially-available-stealth-bitcoinlitecoin-mining-tool>

[-spotted-in-the-wild/](#)

16.

<http://blog.webroot.com/2013/07/23/deceptive-media-player-update-ads-expose-users-to-the-rogue-video-do>

[wnloaderbundlore-potentially-unwanted-application-pua/](#)

17.

<http://blog.webroot.com/2013/07/24/newly-launched-http-based-botnet-setup-as-a-service-empowers-novice-cybercriminals-with-bulletproof-hosting-capabilities/>

18.

<http://blog.webroot.com/2013/07/25/fake-copy-of-vodafone-u-k-contract-your-monthly-vodafone-bill-is-read-ynew-mms-received-themed-emails-lead-to-malware/>

19. <http://blog.webroot.com/2013/07/26/rogue-ads-lead-to-the-free-player-win32somoto-potentially-unwanted-application-pua/>

20.

<http://blog.webroot.com/2013/07/29/how-much-does-it-cost-to-buy-one-thousand-russian-eastern-european-ba>

[343](#)

[sed-malware-infected-hosts/](#)

21. <http://blog.webroot.com/2013/07/30/custom-usb-sticks-bypassing-windows-7s-autorun-protection-measure-going-mainstream/>

22.

<http://blog.webroot.com/2013/07/31/diy-commercially-available-automatic-web-site-hacking-as-a-service-s-potted-in-the-wild/>

23. <http://ddanchev.blogspot.com/>

24. <http://twitter.com/danchodanchev>

344



Dissecting a Sample Russian Business Network (RBN) Contract/Agreement Through the Prism of RBN's

AbdAllah Franchise (2013-08-10 21:10)

[1]**The Russian Business Network (RBN)**, is perhaps the most speculated, buzzed about, cybercrime enterprise in

the World, a poster child for fraudulent activity 'streaming' from 'Mother Russia', in the eyes of respected/novice

security/cybercrime researchers across the globe.

However, what a huge percentage of the researchers who're just catching up with its '[2]**fraudulent perfor-**

mance metrics' over the years, don't realize, is how a newly emerged bulletproof hosting provider, managed to end

up, as the World's most prolific source of fraudulent/malicious activity.

Hint: Basic business concepts like franchising, signalling the early stages of the modernization/professionalization of

cybercrime, where being the benchmark has had a direct inspirational impact in the 'hearts and minds' of current

and potential cybercriminals, then and now.

Case in point is [3]**Abdallah Internet Hizmetleri also known as AbdAllah (VN)**, an ex-RBN darling relying on

the franchise business concept.

In this post, I'll discuss a sample contract/contractual agreement that every one of its customers had to sign

before doing business with them, which in the broader context leads to a situation, where while the franchise is

publicly advertising the bulletproof hosting services for trojans, exploits, warez, adult content, drop projects, botnets

345

and spam, it's explicitly forbidding such activities – with some visible exceptions – in its contractual agreement.

What does this mean? It means that the Russian Business Network, the benchmark for the majority of ex/currently

active bulletproof hosting providers, has been (legally) forwarding the responsibility for the fraudulent activity

to its customers, in between reserving the right to act and deactivate their accounts if they ever violate the

agreement/contract. The first thing that comes to my mind when it comes to the RBN 'reaction' in a socially

oriented manner, are the infamous [4]**RBN Fake Account Suspended Notices**, and that's just for starters, indicating a deteriorated understanding of malicious/fraudulent activity, with high profit margins in mind.

Let's go through the contract/agreement that every customer used to sign, before doing cybercrime-friendly

business with them, both in original Russian, and automatically translated in English.

Sample AbdAllah (VN) Contractual Bulletproof Hosting Agreement/Contract in Russian:

1. ПРЕДМЕТ ДОГОВОРА

1.1. Заказчик поручает, а ИСПОЛНИТЕЛЬ берет на себя обязательства по размещению и/или регистрации

виртуального сервера ЗАКАЗЧИКА в сети Интернет.

2. УСЛОВИЯ ВЫПОЛНЕНИЯ ДОГОВОРА

2.1.

По заключению настоящего договора ИСПОЛНИТЕЛЬ производит первоначальную установку

и настройку виртуального сервера и обеспечивает ЗАКАЗЧИКА необходимой информацией для

администрирования виртуального сервера.

2.2.

ИСПОЛНИТЕЛЬ обеспечивает доступ в сети Интернет к виртуальному серверу, а так же

работоспособность всех доступных сервисов ЗАКАЗЧИКА круглосуточно в течение семи дней в неделю.

3. ЦЕНЫ И ПОРЯДОК ОПЛАТЫ

3.1.

Стоимость и порядок оплаты работ по настоящему договору на момент его заключения

определяется в соответствии с действующими условиями, распространяемыми сотрудниками по E-Mail и/или ICQ.

3.2.

Оплата вносится ЗАКАЗЧИКОМ в счет оплаты услуги поддержки виртуального веб-сервера

ИСПОЛНИТЕЛЕМ. ИСПОЛНИТЕЛЬ вправе приостановить предоставление услуг при отрицательном состоянии счета.

3.3.

Все выделенные серверы предоставляются в состоянии UNMANAGED, т.е администраторы

ИСПОЛНИТЕЛЯ могут, но не ОБЯЗАНЫ настраивать арендуемый сервер. За любую настройку сервера

ЗАКАЗЧИКА, либо скриптов на нём - взимается плата в размере 50 USD/за 1 час работы администратора

ИСПОЛНИТЕЛЯ по Вашему вопросу, минимум пол часа. Полное администрирование сервера специалистами

ИСПОЛНИТЕЛЯ стоит 250 USD в месяц.

Бесплатно осуществляется перезагрузка сервер (если нет

автоматической формы для этого).

3.4. В случае не оплаты услуг ЗАКАЗЧИКОМ в последний день биллингового периода, данные ЗАКАЗЧИКА

удаляются по наступлению новых суток без возврата. В случае виртуального хостинга удаляется

аккаунт и все бэкапы данного аккаунта, в случае аренды сервера (dedicated или vps) сервер снимается с

обслуживания, форматируются жесткие диски.

4. ОТВЕТСТВЕННОСТЬ СТОРОН

346

4.1.

ИСПОЛНИТЕЛЬ не несет ответственности перед ЗАКАЗЧИКОМ или третьими сторонами за

любые задержки, прерывания, ущерб или потери, происходящие из-за:

(а) дефектов в любом электронном или механическом оборудовании, не принадлежащем ИСПОЛНИТЕЛЮ;

(б) проблем при передаче данных или соединении, произошедших не по вине ИСПОЛНИТЕЛЯ ;

(в) вследствие обстоятельств непреодолимой силы в общепринятом смысле, т.е. чрезвычайными силами

и непредотвратимыми обстоятельствами, не подлежащими разумному контролю;

(г) давление властей.

4.2. При расторжении Договора по инициативе ЗАКАЗЧИКА, неиспользованная часть аванса ЗАКАЗЧИКУ не

возвращается.

4.3.

ИСПОЛНИТЕЛЬ оставляет за собой право приостановить обслуживание ЗАКАЗЧИКА или

расторгнуть договор в безусловном порядке без возвращения средств заказчику в следующих случаях:

- размещение детской порнографии и зоофилии в любом виде;

- попытки взлома, несанкционированного проникновения на сервер, в аккаунты других клиентов,

попытки порчи оборудования или программного обеспечения;

- попытки взлома правительственных организаций в любом виде;

- попытки спама любого рода с наших серверов виртуального хостинга, кроме как через соксы;

- попытки фишинга банков (кража денег);

- размещение информации по торговле оружием и наркотиками, торговля людьми или органами

людей, вызывающие межнациональную и религиозную рознь, призывающую к войне и насилию;

- неоправданная перегрузка вычислительных мощностей сервера виртуального хостинга

(допускается

использовать не более 5 % мощности процессора и не более 128Мб оперативной памяти сервера);

- попытки взлома с серверов (dedicated и виртуальный хостинг) - серверы, которые расположены

рядом в стойке, либо клиентов этой же страны, где расположен сервер;

- оскорбление в любой форме сотрудников сервиса.

4.4. ИСПОЛНИТЕЛЬ не отвечает за содержание информации, размещаемой ЗАКАЗЧИКОМ.

4.5. ИСПОЛНИТЕЛЬ не будет нести ответственности за любые затраты или ущерб, прямо или косвенно

возникшие в результате использования услуги вэб хостинга.

4.6. MoneyBack за выделенный сервер возможен только в том случае, если недоступность данного сервера

происходит по вине ИСПОЛНИТЕЛЯ, ввиду того, что ИСПОЛНИТЕЛЬ оплачиваем полную стоимость сервера

в Дата-Центр. Также возможна замена сервера.

4.7.

Размещение сайтов ЗАКАЗЧИКА, рекламируемых SPAMом на серверах ИСПОЛНИТЕЛЯ (как

виртуального хостинга, так и dedicated) оплачивается отдельно из расчета объема писем.

При

объёмах от 5млн до 10млн =1000 USD - 1500 USD в месяц за сервер в Китае или ГонгКонге, либо 150 USD

неделя или 500 USD в месяц за виртуальный хостинг, более 10-20 млн. = 200 USD неделя либо 2000 \$ за

347

выделенный сервер.

4.8. ИСПОЛНИТЕЛЬ обязуется делать ежедневные резервные копии аккаунта ЗАКАЗЧИКА на сторонний сервер (только виртуальный хостинг).

4.9.

ИСПОЛНИТЕЛЬ обязуется решать самостоятельно все жалобы (абузы/abuse), не привлекая к

этому ЗАКАЗЧИКА и без вмешательства в данные ЗАКАЗЧИКА. ИСПОЛНИТЕЛЬ не решает жалобы

(абузы/abuse) от полиции, крупных правительственных организаций и VerSign.

4.10.

ИСПОЛНИТЕЛЬ не дает никаких гарантий, что домен ЗАКАЗЧИКА не будет заблокирован по

любым причинам, а особенно таким как любой вид SPAMa, fraud, phishing и т.п.

5. КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ

5.1. Стороны обязуются без обоюдного согласия не передавать третьим лицам либо использовать иным

способом, не предусмотренным условиями Договора, организационно-технологическую, коммерческую,

финансовую и иную информацию, составляющую секрет для любой из сторон (далее - "конфиденциальная

информация") при условии, что:

- такая информация имеет действительную или потенциальную коммерческую ценность в силу ее

неизвестности третьим лицам;

- к такой информации нет свободного доступа на законном основании;

- обладатель такой информации принимает надлежащие меры к обеспечению ее конфиденциальности.

5.2. Стороны обязуются, без обоюдного согласия, не передавать третьим лицам сведения о содержании

и условиях Договора.

5.3.

ИСПОЛНИТЕЛЬ обязуется предотвращать запись логов на серверах виртуального хостинга и

маршрутизирующем оборудовании.

5.4. Будьте внимательны, сотрудники ИСПОЛНИТЕЛЯ не запрашивают пароли от аккаунтов виртуального

хостинга и выделенных серверов. Исключением является ситуация, когда ЗАКАЗЧИК просить произвести какие-либо работы на его Выделенном Сервере.

348



Automatically translated Russian Business Network (RBN) Contractual Agreement/Contract:

1. SUBJECT OF CONTRACT

1.1.

Customer Requests, but ARTIST is committed to the placement and / or registration CUSTOMER virtual server on the Internet.

2. CONDITIONS OF IMPLEMENTATION OF THE TREATY

2.1. At the conclusion of this treaty ARTIST produces initial setup and configuration of the virtual server and provides the necessary information for CUSTOMER virtual server administration.

2.2. ARTIST provides access to the Internet to the virtual server, as well as efficiency of all available services CUSTOMER day seven days a week.

3. PRICES AND ORDER OF PAYMENT

3.1. Cost and arrangements of works under this contract at the time of its conclusion is determined in accor-

dance with existing conditions, the staff distributed by E-Mail and / or ICQ.

3.2.

Payment is made ZAKAZCHIKOM as payment services support virtual web server ISPOLNITELEM. ARTIST

349

right to suspend the provision of services at a negative status of the account.

3.3. All dedicated servers are provided in a position UNMANAGED ie ISPOLNITELYA administrators can, but not

OBYAZANY tune rented server. For any server setup CUSTOMER or scripts on it - charge of \$ 50 USD / for 1 hour

administrator ISPOLNITELYA to your question, at least half an hour. The full server administration specialists

ISPOLNITELYA worth USD 250 per month. Free done rebooting the server (if not automatic form for this).

3.4. If no payment ZAKAZCHIKOM bill on the last day of the period, the data are removed CUSTOMER new of-

fensive on days without reciprocating. In the case of virtual hosting account and removed all of your backups, in case the rental server (dedicated or vps) server is removed from service, formatted hard drives.

4. RESPONSIBILITY OF PARTIES

4.1. ARTIST no responsibility to ZAKAZCHIKOM or third parties for any delays, interruptions, damage or losses

that occur because of:

(a) defects in any electronic or mechanical equipment, not belonging ISPOLNITELYU;

(b) problems in the transfer of data or connection that occurred through no fault ISPOLNITELYA;

(c) due to force majeure circumstances, in the conventional sense, that is, nepredotvratimymi forces and emergency

circumstances, not subject to reasonable control;

(g) pressure from the authorities.

4.2. At the dissolution of the Treaty on the initiative CUSTOMER, ZAKAZCHIKU unused portion of the advance is not refundable.

4.3. ARTIST reserves the right to suspend or terminate CUSTOMER service contract in order without the un-

conditional return of customer funds in the following cases:

- Locating and zoofilii child pornography in any form;

- attempted burglary, unauthorized entry to the server, in the accounts of other customers, trying to dam-

age equipment or software;

- attempted burglary governmental organizations in any form;

- spam attempts of any kind from our servers hosting virtual except through SOCKS;**
- phishing attempts banks (stealing money);**
- posting on the arms trade and drug trafficking, or human organs, causing inter-ethnic and religious discord, calling for war and violence;**
- unjustified computing power overload virtual server hosting (which is allowed to use no more than 5 % of CPU capacity, and no more than 128 MB of RAM server);**
- attempted burglary of servers (and dedicated virtual hosting) - servers, which are located next to the rack, a customer in the same country where the server;**
- insulting to any form of service personnel.**

4.4. ARTIST is not responsible for the content of the information posted ZAKAZCHIKOM.

350

4.5. ARTIST shall not be liable for any costs or damages arising directly or indirectly from the use of Web hosting services.

4.6. MoneyBack for dedicated server is possible only in case the inaccessibility of the fault occurs on the server

ISPOLNITELYA, because ARTIST pay for the full cost of a server in Data Center. Also possible replacement server.

4.7.

Placing sites CUSTOMER advertised on servers ISPOLNITELYA SPAM (as virtualnogo hosting, and dedicated) is charged separately at the rate of the volume of letters. With volume of 5 million to 10 million USD = 1000

- 1500 USD per month for the server in China or Gong Konge or 150 USD week, or 500 USD per month for a virtual

hosting, a 10-20 million = 200 USD week, or \$ 2000 for a dedicated server.

4.8. ARTIST undertakes to do daily backups CUSTOMER account for the third-party server (only virtual hosting).

4.9. ARTIST undertakes to decide all complaints (abuzy / abuse), are not engaging in the CUSTOMER and

without interference in the CUSTOMER data. ARTIST does not solve complaints (abuzy / abuse) from the police,

government organizations and major VerSign.

4.10. ARTIST gives no guarantees that the domain CUSTOMER not be blocked for any reason, but especially like any kind of SPAM, fraud, phishing, etc.

5. CONFIDENTIAL INFORMATION

5.1. The Parties undertake without the unanimous consent not to transfer to third parties or used in any other

way other than prescribed conditions Treaty, organizational and technological, commercial, financial and other

information, which is the secret to any of the parties (hereinafter - "confidential information"), provided that:

- this information is actual or potential commercial value by virtue of its unknown third parties;*
- to such information no free access to the lawful;*
- holds such information shall take appropriate steps to ensure its confidentiality.*

5.2. The Parties undertake, without unanimous consent, not to transfer to third parties about the content and conditions of the Treaty.

5.3. ARTIST undertakes to prevent logging on servers and virtual hosting routing equipment.

5.4.

Be careful, do not require employees ISPOLNITELYA passwords from virtual hosting accounts and dedi-

cated servers. The exception is when CUSTOMER request to any work for his Vydelennom Server.

Excluding the direct offering of managed servers for spam sending in the actual agreement/contract, and the fact

that their abuse department is virtually non-existent, the contact explicitly prohibits related malicious/fraudulent

activity. Naturally, that's not the case when AbdAllah (VN) used to advertise its bulletproof hosting service across

cybercrime-friendly communities, "back in the day":

351



In 2013, despite the overall availability of RBN-like bulletproof hosting providers, cybercriminals continue experi-

menting with abusing legitimate infrastructure in an attempt to mitigate the risk of having their activities exposed.

Various cases throughout the last couple of years include:

- [5]Cybercriminals use Twitter, LinkedIn, Baidu, MSDN as command and control infrastructure
- [6]RSA: Banking trojan uses social network as command and control server
- [7]Trojan.Whitewell: What's your (bot) Facebook Status Today?
- [8]Twitter-based Botnet Command Channel
- [9]Google Groups Trojan
- [10]Zeus crimeware using Amazon's EC2 as command and control server

The "best" is yet to come.

This post has been reproduced from [11]Dancho Danchev's blog. Follow him [12]on Twitter.

1.

<https://www.google.com/#bav=&q=site:ddanchev.blogspot.com+RBN>

2. <http://www.shadowserver.org/wiki/uploads/Information/RBN-AS40989.pdf>
3. http://www.shadowserver.org/wiki/uploads/Information/RBN_Rizing.pdf
4. <http://ddanchev.blogspot.com/2008/01/rbns-fake-account-suspended-notices.html>
5. <http://www.zdnet.com/blog/security/cybercriminals-use-twitter-linkedin-baidu-msdn-as-command-and-control-infrastructure/11210>
6. <http://www.zdnet.com/blog/security/rsa-banking-trojan-uses-social-network-as-command-and-control-server/6877>
7. <http://www.symantec.com/connect/blogs/trojanwhitewell-what-s-your-bot-facebook-status-today>
8. <http://www.arbornetworks.com/asert/2009/08/twitter-based-botnet-command-channel/>
9. <http://www.symantec.com/connect/blogs/google-groups-trojan>
10. <http://www.zdnet.com/blog/security/zeus-crimeware-using-amazons-ec2-as-command-and-control-server/5110>
11. <http://ddanchev.blogspot.com/>
12. <http://twitter.com/danchodanchev>



Dissecting a Sample Russian Business Network (RBN) Contract/Agreement Through the Prism of RBN's

AbdAllah Franchise (2013-08-10 21:10)

[1]**The Russian Business Network (RBN)**, is perhaps the most speculated, buzzed about, cybercrime enterprise in

the World, a poster child for fraudulent activity 'streaming' from 'Mother Russia', in the eyes of respected/novice

security/cybercrime researchers across the globe.

However, what a huge percentage of the researchers who're just catching up with its '[2]**fraudulent perfor-**

mance metrics' over the years, don't realize, is how a newly emerged bulletproof hosting provider, managed to end

up, as the World's most prolific source of fraudulent/malicious activity.

Hint: Basic business concepts like franchising, signalling the early stages of the modernization/professionalization of

cybercrime, where being the benchmark has had a direct inspirational impact in the 'hearts and minds' of current

and potential cybercriminals, then and now.

Case in point is [3]**Abdallah Internet Hizmetleri also known as AbdAllah (VN)**, an ex-RBN darling relying on

the franchise business concept.

In this post, I'll discuss a sample contract/contractual agreement that every one of its customers had to sign before doing business with them, which in the broader context leads to a situation, where while the franchise is publicly advertising the bulletproof hosting services for trojans, exploits, warez, adult content, drop projects, botnets

353

and spam, it's explicitly forbidding such activities – with some visible exceptions – in its contractual agreement.

What does this mean? It means that the Russian Business Network, the benchmark for the majority of ex/currently

active bulletproof hosting providers, has been (legally) forwarding the responsibility for the fraudulent activity

to its customers, in between reserving the right to act and deactivate their accounts if they ever violate the

agreement/contract. The first thing that comes to my mind when it comes to the RBN 'reaction' in a socially

oriented manner, are the infamous [4]**RBN Fake Account Suspended Notices**, and that's just for starters, indicating a deteriorated understanding of malicious/fraudulent activity, with high profit margins in mind.

Let's go through the contract/agreement that every customer used to sign, before doing cybercrime-friendly

business with them, both in original Russian, and automatically translated in English.

Sample AbdAllah (VN) Contractual Bulletproof Hosting Agreement/Contract in Russian:

1. ПРЕДМЕТ ДОГОВОРА

1.1. Заказчик поручает, а ИСПОЛНИТЕЛЬ берет на себя обязательства по размещению и/или регистрации

виртуального сервера ЗАКАЗЧИКА в сети Интернет.

2. УСЛОВИЯ ВЫПОЛНЕНИЯ ДОГОВОРА

2.1.

По заключению настоящего договора ИСПОЛНИТЕЛЬ производит первоначальную установку

и настройку виртуального сервера и обеспечивает ЗАКАЗЧИКА необходимой информацией для

администрирования виртуального сервера.

2.2.

ИСПОЛНИТЕЛЬ обеспечивает доступ в сети Интернет к виртуальному серверу, а так же

работоспособность всех доступных сервисов ЗАКАЗЧИКА круглосуточно в течение семи дней в неделю.

3. ЦЕНЫ И ПОРЯДОК ОПЛАТЫ

3.1.

Стоимость и порядок оплаты работ по настоящему договору на момент его заключения

определяется в соответствии с действующими условиями, распространяемыми сотрудниками по E-Mail и/или ICQ.

3.2.

Оплата вносится ЗАКАЗЧИКОМ в счет оплаты услуги поддержки виртуального веб-сервера

ИСПОЛНИТЕЛЕМ. ИСПОЛНИТЕЛЬ вправе приостановить предоставление услуг при отрицательном состоянии счета.

3.3.

Все выделенные серверы предоставляются в состоянии UNMANAGED, т.е администраторы

ИСПОЛНИТЕЛЯ могут, но не ОБЯЗАНЫ настраивать арендуемый сервер. За любую настройку сервера

ЗАКАЗЧИКА, либо скриптов на нём - взимается плата в размере 50 USD/за 1 час работы администратора

ИСПОЛНИТЕЛЯ по Вашему вопросу, минимум пол часа. Полное администрирование сервера специалистами

ИСПОЛНИТЕЛЯ стоит 250 USD в месяц.

Бесплатно осуществляется перезагрузка сервер (если нет

автоматической формы для этого).

3.4. В случае не оплаты услуг ЗАКАЗЧИКОМ в последний день биллингового периода, данные ЗАКАЗЧИКА

удаляются по наступлению новых суток без возврата. В случае виртуального хостинга удаляется

аккаунт и все бэкапы данного аккаунта, в случае аренды сервера (dedicated или vps) сервер снимается с

обслуживания, форматируются жесткие диски.

4. ОТВЕТСТВЕННОСТЬ СТОРОН

354

4.1.

ИСПОЛНИТЕЛЬ не несет ответственности перед ЗАКАЗЧИКОМ или третьими сторонами за

любые задержки, прерывания, ущерб или потери, происходящие из-за:

(а) дефектов в любом электронном или механическом оборудовании, не принадлежащем ИСПОЛНИТЕЛЮ;

(б) проблем при передаче данных или соединении, произошедших не по вине ИСПОЛНИТЕЛЯ ;

(в) вследствие обстоятельств непреодолимой силы в общепринятом смысле, т.е. чрезвычайными силами

и непредотвратимыми обстоятельствами, не подлежащими разумному контролю;

(г) давление властей.

4.2. При расторжении Договора по инициативе ЗАКАЗЧИКА, неиспользованная часть аванса ЗАКАЗЧИКУ не

возвращается.

4.3.

ИСПОЛНИТЕЛЬ оставляет за собой право приостановить обслуживание ЗАКАЗЧИКА или

расторгнуть договор в безусловном порядке без возвращения средств заказчику в следующих случаях:

- размещение детской порнографии и зоофилии в любом виде;

- попытки взлома, несанкционированного проникновения на сервер, в аккаунты других клиентов,

попытки порчи оборудования или программного обеспечения;

- попытки взлома правительственных организаций в любом виде;

- попытки спама любого рода с наших серверов виртуального хостинга, кроме как через соксы;

- попытки фишинга банков (кража денег);

- размещение информации по торговле оружием и наркотиками, торговля людьми или органами

людей, вызывающие межнациональную и религиозную рознь, призывающую к войне и насилию;

- неоправданная перегрузка вычислительных мощностей сервера виртуального хостинга

(допускается

использовать не более 5 % мощности процессора и не более 128Мб оперативной памяти сервера);

- попытки взлома с серверов (dedicated и виртуальный хостинг) - серверы, которые расположены

рядом в стойке, либо клиентов этой же страны, где расположен сервер;

- оскорбление в любой форме сотрудников сервиса.

4.4. ИСПОЛНИТЕЛЬ не отвечает за содержание информации, размещаемой ЗАКАЗЧИКОМ.

4.5. ИСПОЛНИТЕЛЬ не будет нести ответственности за любые затраты или ущерб, прямо или косвенно

возникшие в результате использования услуги вэб хостинга.

4.6. MoneyBack за выделенный сервер возможен только в том случае, если недоступность данного сервера

происходит по вине ИСПОЛНИТЕЛЯ, ввиду того, что ИСПОЛНИТЕЛЬ оплачиваем полную стоимость сервера

в Дата-Центр. Также возможна замена сервера.

4.7.

Размещение сайтов ЗАКАЗЧИКА, рекламируемых SPAMом на серверах ИСПОЛНИТЕЛЯ (как

виртуального хостинга, так и dedicated) оплачивается отдельно из расчета объема писем.

При

объёмах от 5млн до 10млн =1000 USD - 1500 USD в месяц за сервер в Китае или ГонгКонге, либо 150 USD

неделя или 500 USD в месяц за виртуальный хостинг, более 10-20 млн. = 200 USD неделя либо 2000 \$ за

355

выделенный сервер.

4.8. ИСПОЛНИТЕЛЬ обязуется делать ежедневные резервные копии аккаунта ЗАКАЗЧИКА на сторонний сервер (только виртуальный хостинг).

4.9.

ИСПОЛНИТЕЛЬ обязуется решать самостоятельно все жалобы (абузы/abuse), не привлекая к

этому ЗАКАЗЧИКА и без вмешательства в данные ЗАКАЗЧИКА. ИСПОЛНИТЕЛЬ не решает жалобы

(абузы/abuse) от полиции, крупных правительственных организаций и VerSign.

4.10.

ИСПОЛНИТЕЛЬ не дает никаких гарантий, что домен ЗАКАЗЧИКА не будет заблокирован по

любым причинам, а особенно таким как любой вид SPAMa, fraud, phishing и т.п.

5. КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ

5.1. Стороны обязуются без обоюдного согласия не передавать третьим лицам либо использовать иным

способом, не предусмотренным условиями Договора, организационно-технологическую, коммерческую,

финансовую и иную информацию, составляющую секрет для любой из сторон (далее - "конфиденциальная

информация") при условии, что:

- такая информация имеет действительную или потенциальную коммерческую ценность в силу ее

неизвестности третьим лицам;

- к такой информации нет свободного доступа на законном основании;

- обладатель такой информации принимает надлежащие меры к обеспечению ее конфиденциальности.

5.2. Стороны обязуются, без обоюдного согласия, не передавать третьим лицам сведения о содержании

и условиях Договора.

5.3.

ИСПОЛНИТЕЛЬ обязуется предотвращать запись логов на серверах виртуального хостинга и

маршрутизирующем оборудовании.

5.4. Будьте внимательны, сотрудники ИСПОЛНИТЕЛЯ не запрашивают пароли от аккаунтов виртуального

хостинга и выделенных серверов. Исключением является ситуация, когда ЗАКАЗЧИК просить произвести какие-либо работы на его Выделенном Сервере.

356



Automatically translated Russian Business Network (RBN) Contractual Agreement/Contract:

1. SUBJECT OF CONTRACT

1.1.

Customer Requests, but ARTIST is committed to the placement and / or registration CUSTOMER virtual server on the Internet.

2. CONDITIONS OF IMPLEMENTATION OF THE TREATY

2.1. At the conclusion of this treaty ARTIST produces initial setup and configuration of the virtual server and provides the necessary information for CUSTOMER virtual server administration.

2.2. ARTIST provides access to the Internet to the virtual server, as well as efficiency of all available services CUSTOMER day seven days a week.

3. PRICES AND ORDER OF PAYMENT

3.1. Cost and arrangements of works under this contract at the time of its conclusion is determined in accor-

dance with existing conditions, the staff distributed by E-Mail and / or ICQ.

3.2.

Payment is made ZAKAZCHIKOM as payment services support virtual web server ISPOLNITELEM. ARTIST

357

right to suspend the provision of services at a negative status of the account.

3.3. All dedicated servers are provided in a position UNMANAGED ie ISPOLNITELYA administrators can, but not

OBYAZANY tune rented server. For any server setup CUSTOMER or scripts on it - charge of \$ 50 USD / for 1 hour

administrator ISPOLNITELYA to your question, at least half an hour. The full server administration specialists

ISPOLNITELYA worth USD 250 per month. Free done rebooting the server (if not automatic form for this).

3.4. If no payment ZAKAZCHIKOM bill on the last day of the period, the data are removed CUSTOMER new of-

fensive on days without reciprocating. In the case of virtual hosting account and removed all of your backups, in case the rental server (dedicated or vps) server is removed from service, formatted hard drives.

4. RESPONSIBILITY OF PARTIES

4.1. ARTIST no responsibility to ZAKAZCHIKOM or third parties for any delays, interruptions, damage or losses

that occur because of:

(a) defects in any electronic or mechanical equipment, not belonging ISPOLNITELYU;

(b) problems in the transfer of data or connection that occurred through no fault ISPOLNITELYA;

(c) due to force majeure circumstances, in the conventional sense, that is, nepredotvratimymi forces and emergency

circumstances, not subject to reasonable control;

(g) pressure from the authorities.

4.2. At the dissolution of the Treaty on the initiative CUSTOMER, ZAKAZCHIKU unused portion of the advance is not refundable.

4.3. ARTIST reserves the right to suspend or terminate CUSTOMER service contract in order without the un-

conditional return of customer funds in the following cases:

- Locating and zoofilii child pornography in any form;

- attempted burglary, unauthorized entry to the server, in the accounts of other customers, trying to dam-

age equipment or software;

- attempted burglary governmental organizations in any form;

- spam attempts of any kind from our servers hosting virtual except through SOCKS;**
- phishing attempts banks (stealing money);**
- posting on the arms trade and drug trafficking, or human organs, causing inter-ethnic and religious discord, calling for war and violence;**
- unjustified computing power overload virtual server hosting (which is allowed to use no more than 5 % of CPU capacity, and no more than 128 MB of RAM server);**
- attempted burglary of servers (and dedicated virtual hosting) - servers, which are located next to the rack, a customer in the same country where the server;**
- insulting to any form of service personnel.**

4.4. ARTIST is not responsible for the content of the information posted ZAKAZCHIKOM.

358

4.5. ARTIST shall not be liable for any costs or damages arising directly or indirectly from the use of Web hosting services.

4.6. MoneyBack for dedicated server is possible only in case the inaccessibility of the fault occurs on the server

ISPOLNITELYA, because ARTIST pay for the full cost of a server in Data Center. Also possible replacement server.

4.7.

Placing sites CUSTOMER advertised on servers ISPOLNITELYA SPAM (as virtualnogo hosting, and dedicated) is charged separately at the rate of the volume of letters. With volume of 5 million to 10 million USD = 1000

- 1500 USD per month for the server in China or Gong Konge or 150 USD week, or 500 USD per month for a virtual

hosting, a 10-20 million = 200 USD week, or \$ 2000 for a dedicated server.

4.8. ARTIST undertakes to do daily backups CUSTOMER account for the third-party server (only virtual hosting).

4.9. ARTIST undertakes to decide all complaints (abuzy / abuse), are not engaging in the CUSTOMER and

without interference in the CUSTOMER data. ARTIST does not solve complaints (abuzy / abuse) from the police,

government organizations and major VerSign.

4.10. ARTIST gives no guarantees that the domain CUSTOMER not be blocked for any reason, but especially like any kind of SPAM, fraud, phishing, etc.

5. CONFIDENTIAL INFORMATION

5.1. The Parties undertake without the unanimous consent not to transfer to third parties or used in any other

way other than prescribed conditions Treaty, organizational and technological, commercial, financial and other

information, which is the secret to any of the parties (hereinafter - "confidential information"), provided that:

- this information is actual or potential commercial value by virtue of its unknown third parties;*
- to such information no free access to the lawful;*
- holds such information shall take appropriate steps to ensure its confidentiality.*

5.2. The Parties undertake, without unanimous consent, not to transfer to third parties about the content and conditions of the Treaty.

5.3. ARTIST undertakes to prevent logging on servers and virtual hosting routing equipment.

5.4.

Be careful, do not require employees ISPOLNITELYA passwords from virtual hosting accounts and dedi-

cated servers. The exception is when CUSTOMER request to any work for his Vydelennom Server.

Excluding the direct offering of managed servers for spam sending in the actual agreement/contract, and the fact

that their abuse department is virtually non-existent, the contact explicitly prohibits related malicious/fraudulent

activity. Naturally, that's not the case when AbdAllah (VN) used to advertise its bulletproof hosting service across

cybercrime-friendly communities, "back in the day":

359



In 2013, despite the overall availability of RBN-like bulletproof hosting providers, cybercriminals continue experi-

menting with abusing legitimate infrastructure in an attempt to mitigate the risk of having their activities exposed.

Various cases throughout the last couple of years include:

- [5]Cybercriminals use Twitter, LinkedIn, Baidu, MSDN as command and control infrastructure
- [6]RSA: Banking trojan uses social network as command and control server
- [7]Trojan.Whitewell: What's your (bot) Facebook Status Today?
- [8]Twitter-based Botnet Command Channel
- [9]Google Groups Trojan
- [10]Zeus crimeware using Amazon's EC2 as command and control server

The "best" is yet to come.

This post has been reproduced from [11]Dancho Danchev's blog. Follow him [12]on Twitter.

1.

<https://www.google.com/#bav=&q=site:ddanchev.blogspot.com+RBN>

2. <http://www.shadowserver.org/wiki/uploads/Information/RBN-AS40989.pdf>
3. http://www.shadowserver.org/wiki/uploads/Information/RBN_Rizing.pdf
4. <http://ddanchev.blogspot.com/2008/01/rbns-fake-account-suspended-notices.html>
5. <http://www.zdnet.com/blog/security/cybercriminals-use-twitter-linkedin-baidu-msdn-as-command-and-control-infrastructure/11210>
6. <http://www.zdnet.com/blog/security/rsa-banking-trojan-uses-social-network-as-command-and-control-server/6877>
7. <http://www.symantec.com/connect/blogs/trojanwhitewell-what-s-your-bot-facebook-status-today>
8. <http://www.arbornetworks.com/asert/2009/08/twitter-based-botnet-command-channel/>
9. <http://www.symantec.com/connect/blogs/google-groups-trojan>
10. <http://www.zdnet.com/blog/security/zeus-crimeware-using-amazons-ec2-as-command-and-control-server/5110>
11. <http://ddanchev.blogspot.com/>
12. <http://twitter.com/danchodanchev>



Spamvertised 'Confirmed Facebook Friend Request' Themed Emails Serve Client-Side Exploits

(2013-08-15 14:03)

A currently circulating malicious spam campaign, entices users into thinking that they've received a legitimate ' *Friend Confirmation Request*' on Facebook. In reality thought, the campaign attempts to exploit client-side vulnerabilities,

[1]**CVE-2010-0188** in particular.

Client-side exploits serving URL:

hxxp://facebook.com.n.find-friends.lindoliveryct.net:80/news/facebo

ok-onetime.php?dpheelxa=1l:30:1l:1g:1j

*&pkvby=h &rzuhhh=1h:33:1o:2v:32:1o:2v:1o:1j:1m
&ycxlcvr=1f:1d:1f:1d:1f:1d:1f*

Detection rate for the malicious PDF: [2]MD5: 39326c9a2572078c379eb6494dc326ab - detected by 3 out of

45 antivirus scanners as PDF/Blacole-FAA!39326C9A2572; Exploit:Win32/CVE-2010-0188; Exploit.Script.Pdfka.btvxj

Domain name reconnaissance:

facebook.com.n.find-friends.lindoliveryct.net - 66.230.163.86; 95.111.32.249; 188.134.26.172 - Email: zsuper-

cats@yahoo.com

**Responding to the same IPs (66.230.163.86;
95.111.32.249; 188.134.26.172) are also the followig
malicious**

domains:

actiry.com - Email: stritton@actiry.com

askfox.net - Emal: bovy@askfox.net

bnamecorni.com

briltox.com - Email: lyosha@briltox.com

condalinneuwu37.net

361

condrskajaumaksa66.net

cyberflorists.su - Email: mipartid@gmx.com

evishop.net - Email: hardwicke@evishop.net

exnihujatreetrichmand77.net

gondorskiedelaahueteбанj88.net

gotoraininthecharefare88.net

liliputttt9999.info - Email: dolgopoliy.alexei@yandex.ru

lucams.net - Email: renault@lucams.net

micnetwork100.com - Email: 369258wq@sina.com

musicstudioseattle.net- Email: rexona1948@live.com

nvufvwieg.com - Email: 369258wq@sina.com

partyspecialty.su - Email: mipartid@gmx.com

pinterest.com.onsayoga.net

quill.com.account.settings.musicstudioseattle.net

seoworkblog.net - Email: mendhamnewjersey@linuxmail.org

seoworkblog.net

tigerdirect.com.secure.orderlogin.asp.palmer-ford.net

tor-connect-secure.com - Email: 369258wq@sina.com

vip-proxy-to-tor.com

Name servers used in these campaigns:

*Name Server: NS1.TEMPLATESWELL.NET - 94.249.254.48 -
Email: freejob62@rocketmail.com*

*Name Server: NS1.THEGALAXYATWORK.COM - 94.249.254.48
- Email: samyideaa@yahoo.com*

*Name Server: NS1.MOBILE-UNLOCKED.NET - 91.227.220.104
- Email: usalifecoach47@mail.com*

Name Server: NS2.MOBILE-UNLOCKED.NET - 32.100.2.98

Name Server: NS1.KNEESLAPPERZ.NET

*Name Server: NS1.MEDUSASCREAM.NET - 37.247.108.250 -
Email: m_mybad@yahoo.com*

*Name Server: NS1.CREDIT-FIND.NET - 194.209.82.222 -
Email: mendhamnewjersey@linuxmail.org*

*Name Server: NS1.GONULPALACE.NET - 194.209.82.222 -
Email: mitinsider@live.com*

*Name Server: NS1.NAMASTELEARNING.NET - 93.178.205.234
- Email: minelapse2001@outlook.com*

Name Server: NS2.NAMASTELEARNING.NET - 205.28.29.52

**The following malicious MD5s are also known to have
phoned back to the same IPs/were downloaded from
the same IPs in the past:**

MD5: e08c8ed751a3fc36bc966e47b76e2863

MD5: f507b822651d2fbc82a98e4cc7f735a2

MD5: e08c8ed751a3fc36bc966e47b76e2863

MD5: f88d6a7381c0bbac1b1558533cfd62

MD5: 11be39e64c9926ea39e6b2650624dab4

MD5: ea893fb04cc536ff692cc3177db7e66f

MD5: c8f8b4c0fced61f8a4d3b2854279b4ef

MD5: 93bae01631d10530a7bac7367458abea

MD5: 199b8cf0ffd607787907b68c9ebecc8b

MD5: 6b1bef6fb45f5c2d8b46a6eb6a2d5834

MD5: 9eb6ed284284452f7a1e4e3877dded2d

MD5: efacf1c2c6b33f658c3df6a3ed170e2d

MD5: 7c70d5051826c9c93270b8c7fc9d276f

MD5: dcb378d6033eed2e01ff9ab8936050a0

MD5: 8556f98907fd74be9a9c1b3bf602f869

362

This post has been reproduced from [3]Dancho Danchev's blog. Follow him [4]on Twitter.

1. <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0188>

2. <https://www.virustotal.com/en/file/667fc839167456a70f22cf5c6ef8f0291d4e1399374219469f56472251ec58af/analysis/1376565463/>

3. <http://ddanchev.blogspot.com/>

4. <http://twitter.com/danchodanchev>

363



Spamvertised 'Confirmed Facebook Friend Request' Themed Emails Serve Client-Side Exploits

(2013-08-15 14:03)

A currently circulating malicious spam campaign, entices users into thinking that they've received a legitimate ' *Friend Confirmation Request*' on Facebook. In reality though, the campaign attempts to exploit client-side vulnerabilities,

[1]**CVE-2010-0188** in particular.

Client-side exploits serving URL:

*hxxp://facebook.com.n.find-
friends.lindoliveryct.net:80/news/facebo*

ok-onetime.php?dpheelxa=1l:30:1l:1g:1j

*&pkvby=h &rzuhhh=1h:33:1o:2v:32:1o:2v:1o:1j:1m
&ycxlcvr=1f:1d:1f:1d:1f:1d:1f*

**Detection rate for the malicious PDF: [2]MD5:
39326c9a2572078c379eb6494dc326ab** - detected by 3
out of

45 antivirus scanners as PDF/Blacole-FAA!39326C9A2572;
Exploit:Win32/CVE-2010-0188; Exploit.Script.Pdfka.btvxj

Domain name reconnaissance:

facebook.com.n.find-friends.lindoliveryct.net -
66.230.163.86; 95.111.32.249; 188.134.26.172 - Email:
zsuper-

cats@yahoo.com

**Responding to the same IPs (66.230.163.86;
95.111.32.249; 188.134.26.172) are also the followig
malicious**

domains:

actiry.com - Email: stritton@actiry.com

askfox.net - Emal: bovy@askfox.net

bnamecorni.com

briltox.com - Email: lyosha@briltox.com

condalinneuwu37.net

condrskajaumaksa66.net

cyberflorists.su - Email: mipartid@gmx.com

evishop.net - Email: hardwicke@evishop.net

exnihujatreetrichmand77.net

gondorskiedelaahuetebanj88.net

gotoraininthecharefare88.net

liliputttt9999.info - Email: dolgopoliy.alexei@yandex.ru

lucams.net - Email: renault@lucams.net

micnetwork100.com - Email: 369258wq@sina.com

musicstudioseattle.net- Email: rexona1948@live.com

nvufvwieg.com - Email: 369258wq@sina.com

partyspecialty.su - Email: mipartid@gmx.com

pinterest.com.onsayoga.net

quill.com.account.settings.musicstudioseattle.net

seoworkblog.net - Email: mendhamnewjersey@linuxmail.org

seoworkblog.net

tigerdirect.com.secure.orderlogin.asp.palmer-ford.net

tor-connect-secure.com - Email: 369258wq@sina.com

vip-proxy-to-tor.com

Name servers used in these campaigns:

*Name Server: NS1.TEMPLATESWELL.NET - 94.249.254.48 -
Email: freejob62@rocketmail.com*

*Name Server: NS1.THEGALAXYATWORK.COM - 94.249.254.48
- Email: samyideaa@yahoo.com*

*Name Server: NS1.MOBILE-UNLOCKED.NET - 91.227.220.104
- Email: usalifecoach47@mail.com*

Name Server: NS2.MOBILE-UNLOCKED.NET - 32.100.2.98

Name Server: NS1.KNEESLAPPERZ.NET

*Name Server: NS1.MEDUSASCREAM.NET - 37.247.108.250 -
Email: m_mybad@yahoo.com*

*Name Server: NS1.CREDIT-FIND.NET - 194.209.82.222 -
Email: mendhamnewjersey@linuxmail.org*

*Name Server: NS1.GONULPALACE.NET - 194.209.82.222 -
Email: mitinsider@live.com*

*Name Server: NS1.NAMASTELEARNING.NET - 93.178.205.234
- Email: minelapse2001@outlook.com*

Name Server: NS2.NAMASTELEARNING.NET - 205.28.29.52

**The following malicious MD5s are also known to have
phoned back to the same IPs/were downloaded from**

the same IPs in the past:

MD5: e08c8ed751a3fc36bc966e47b76e2863

MD5: f507b822651d2fbc82a98e4cc7f735a2

MD5: e08c8ed751a3fc36bc966e47b76e2863

MD5: f88d6a7381c0bbac1b1558533cfd62

MD5: 11be39e64c9926ea39e6b2650624dab4

MD5: ea893fb04cc536ff692cc3177db7e66f

MD5: c8f8b4c0fced61f8a4d3b2854279b4ef

MD5: 93bae01631d10530a7bac7367458abea

MD5: 199b8cf0ffd607787907b68c9ebecc8b

MD5: 6b1bef6fb45f5c2d8b46a6eb6a2d5834

MD5: 9eb6ed284284452f7a1e4e3877dded2d

MD5: efacf1c2c6b33f658c3df6a3ed170e2d

MD5: 7c70d5051826c9c93270b8c7fc9d276f

MD5: dcb378d6033eed2e01ff9ab8936050a0

MD5: 8556f98907fd74be9a9c1b3bf602f869

365

Updates will be posted as soon as new developments take place.

1. <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0188>

2. <https://www.virustotal.com/en/file/667fc839167456a70f22cf5c6ef8f0291d4e1399374219469f56472251ec58af/analysis/1376565463/>

The Cost of Anonymizing a Cybercriminal's Internet Activities - Part Three (2013-08-21 20:57)

Over the years, I've been persistently highlighting the abuse of compromised hosts as either 'stepping stones',

or as the primary facilitators for 'island hopping' campaigns, empowering those using them with the necessary

non-attributable 'know-how' to not just anonymize their Internet activities, but also, engineer cyber warfare tensions.

The utilization of hacked/compromised hosts/PCs as 'island hopping' points, or as 'stepping stones', continues

to take place in 2013, with more managed cybercrime-friendly services offering access to compromised hosts

located virtually all over the World, access to which can be bought in a cost-effective manner, thanks to the available

discounts or price discrimination schemes.

Catch up with previous research on the topic:

- [1]The Cost of Anonymizing a Cybercriminal's Internet Activities
- [2]The Cost of Anonymizing a Cybercriminal's Internet Activities - Part Two
- [3]Cybercriminals SQL Inject Cybercrime-friendly Proxies Service
- [4]Malware Infected Hosts as Stepping Stones

- [5] Hacked PCs as 'anonymization stepping-stones' service operates in the open since 2004

- [6] 'Malware-infected hosts as stepping stones' service offers access to hundreds of compromised U.S based

hosts

- [7] New service converts malware-infected hosts into anonymization proxies

What has changed over the years? Is the once thought to be the future of anonymization for cybercrime-friendly

activities, 'proxy chaining' – think chaining of connections between multiple malware-infected hosts – still relevant

today? Or was the concept largely replaced by log and data retention free cybercrime-friendly VPN providers, that

continue popping up on everyone's radar?

Since 2010, a HTTPS-supporting, DIY multiple gates application (proxy which can be a Socks 4/Socks 5 compro-

mised host given it has been properly configured for the purpose) managing, Man-in-the-Middle "attack" performing

– in order to randomize for anonymization purposes – cookie/headers modifying of the requests performed through

the "chaining" of compromised hosts/servers, has been commercially available for cybercriminals to take advantage of.

Let's take a close look at this state of the art gate/proxy chaining cybercrime-friendly application.

Sample screenshots of the application's interface:

367



368



369



370



371



The application's author is also known to have been released custom builds for various cybercrime-friendly forums:

372



Some of its core features include:

[+] HTTPS support for php-gates, needs OpenSSL

[+] Ability to set a password on the gate.

[+] Ability to work with a gate, through any procs (HTTP (S), SOCKS4, SOCKS5).

[+] Working with gated exclusively via the method GET, which provides protection from detection by the log files on

the server.

[+] Ability to set Cookies, transferred during handling to the gate. This is useful for hiding the code in the files of the site gate. Format: "cookie = value; cookie2 = ;"

[+] Processing of each compound is in a separate stream.

[+] Ability to unlimited downloads and uploads of large files (in case of inability to bypass restrictions set `_time_limit` () can download files in a few times, provided support to resume from the target server).

[+] Preprocessing mechanism optimizes queries under HTTP 1.0.

[+] The presence of an encryption key must be specified (purely symbolic encryption to hide traffic from prying eyes), and all data, including the password for the gate are transmitted in encrypted form. Enable / disable the encryption

does not require editing the code gate.

[+] Ability to work with several gates. In this case, each assigned a specific gated User-Agent (assigned by chance)

that does not allow the target site to link together the requests from different gates.

[+] Ability to add a request to the target site header X-Forwarded-For, X-Real-Ip and Via with random IP-addresses (in this case, sites that use mechanisms for determining the visitor's IP address on these titles or used `mod_realip`, will benefit from logging bogus addresses, as these headlines mislead the site administrator).

[+] Ability to select the interface to listen to.

[+] More statistics on network connections, there are different levels of profiling queries (and no logs are written to the file).

[+] Support chains gates.

[+]-Chain of 3 modes:

- Direct sequence (traffic passes through a series of gates that you clearly stated)

373

- Random chain (each request is passed through a randomly builds a chain of gates)

- Casual chain with specific output gate time (similar to the previous mode, except that the final gate remains constant.

[+] Ability to speed up surfing through the chain by local caching IP-addresses.

[+] Support for HTTPS gates are not independent of their number.

[+] Using a cascade encryption - the ability to use any number of gates with different encryption keys.

[+] Built-checker gates.

[+] You can check all the gates at once, or each gate individually when adding / editing.

[+] Built-in gates.

[+] Ability to insert code in the gate pre-generated table of permutations. This eliminates the need to store the

encryption key directly to the Gate, and generate a table for each access to the gate.

[+] Automate the process of creating a masked gate with Cookies

[+] Ability to delete from the code perevodoa lines and tabs.

[+] Ability to set proivolnyh request headers.

[+] Ability to define hosts, which will be sent to a specific heading.

[+] Ability to temporarily activate / deactivate a specific heading.

[+] Gain Control key to 2048 bits (256 bytes) using md5

[+] Complete independence from each other bytes (including the order of the bytes and encrypted block length).

[+] The variable number of rounds of permutations, depending on the key.

[+] Partly salt as XOR'a-byte hash key.

With the ease of assessing a malware-infected host's bandwidth thanks to the overall availability of such an

option among the most popular managed services offering access to such hosts, it shouldn't be surprising to consider

that a potential cybercriminal using this application, would be in a perfect position to create – [8]**in a DIY fashion**

– a stable anonymous network, to further assist him on his way to achieve his fraudulent or purely malicious objectives.

The bottom line? What's the cost of anonymizing a cybercriminal's Internet activities? 1,900 rubles or \$57.53

for the application, in this particular case.

This post has been reproduced from [9]Dancho Danchev's blog. Follow him [10]on Twitter.

1. <http://ddanchev.blogspot.com/2008/10/cost-of-anonymizing-cybercriminals.html>
2. <http://ddanchev.blogspot.com/2009/02/cost-of-anonymizing-cybercriminals.html>
3. <http://ddanchev.blogspot.com/2010/07/cybercriminals-sql-inject-cybercrime.html>
4. <http://ddanchev.blogspot.com/2008/02/malware-infected-hosts-as-stepping.html>
5. <http://blog.webroot.com/2013/03/20/hacked-pcs-as-anonymization-stepping-stones-service-operates-in-the-open-since-2004/>
6. <http://blog.webroot.com/2013/08/02/malware-infected-hosts-as-stepping-stones-service-offers-access-to-hundreds-of-compromised-u-s-based-hosts/>
7. <http://blog.webroot.com/2012/03/02/new-service-converts-malware-infected-hosts-into-anonymization-proxies/>
8. <http://blog.webroot.com/tag/diy/>
9. <http://ddanchev.blogspot.com/>
10. <http://twitter.com/danchodanchev>

Vendor of Scanned Fake IDs, Credit Cards and Utility Bills Targets the French Market Segment

(2013-08-22 18:19)

Continuing the series of blog posts detailing the very latest efficiency/quality/scalability/universal business concepts

oriented underground market propositions for fake IDs, credit cards and utility bills, in this post I'll discuss an example of market segmentation in terms of supplying them, through an ad targeting potential cybercriminals based in France,

or international cybercriminals wanting to enter the French market.

Catch up with previous research on the topic:

- [1] Newly Launched 'Scanned Fake Passports/IDs/Credit Cards/Utility Bills' Service Randomizes and Generates

Unique Fakes On The Fly

- [2] A Peek Inside the Russian Underground Market for Fake Documents/IDs/Passports

What's so special about this underground market proposition, anyway? It's the market segmentation taking place

through the eyes of the vendor, as well as the diversity of scanned .PSD Photoshop templates, the non-modifiable

scanned documents, and the actual availability of physical fake IDs, all of them exclusively targeting the French

market segment.

Sample screenshot of the advertisement:

375



There are several types of vendors contributing to the currently mature state of the market for fake IDs/documents, or to the cybercrime ecosystem in general. Let's discuss the most popular types of market players.

Among the rarest type of such vendors is the experienced one who tends not to advertise at public or com-

mercially accessible cybercrime-friendly communities. Although it would seem fairly logical to assume that the

applied OPSEC (Operational Security) would be directly proportional with the decrease in processed orders since it

would limit the visibility of his services within the cybercrime ecosystem, that's not necessarily the case when quality,

experience, sophisticated, and, of course, high profit margins based on perceived value come into play. In between

the lack of mass advertisements, the vendor would also not list his contact details, and would only do business with cy-

bercriminals with proven reputation within not just the community in question, but also, across the entire ecosystem.

Next are those vendors who'd sacrifice OPSEC, for the sake of reaching as many customers as possible in an

attempt to monetize this market 'touch point' with other prospective cybercriminals. They advertise on public

and on commercially accessible cybercrime-friendly communities, usually have a decent reputation, with generally

positive feedback from their customers, and of course, never fail to 'deliver' what they pitch.

376

There's yet another type of such vendors, worth discussing. It's those who 'populate' a newly launched community with their propositions, and most often target novice cybercriminals with zero understanding of cybercrime

ecosystem reputation dynamics, who are still looking to purchase this desired, but largely commoditized underground

market good.

With more vendors of fake IDs/documents popping up across the entire ecosystem, the series of blog posts

profiling their activities, are prone to expand.

This post has been reproduced from [3]Dancho Danchev's blog. Follow him [4]on Twitter.

1. <http://ddanchev.blogspot.com/2013/07/newly-launched-scanned-fake.html>

2. <http://ddanchev.blogspot.com/2013/05/a-peek-inside-russian-underground.html>

3. <http://ddanchev.blogspot.com/>

4. <http://twitter.com/danchodanchev>

377

Vendor of Scanned Fake IDs, Credit Cards and Utility Bills Targets the French Market Segment

(2013-08-22 18:19)

Continuing the series of blog posts detailing the very latest efficiency/quality/scalability/universal business concepts

oriented underground market propositions for fake IDs, credit cards and utility bills, in this post I'll discuss an example of market segmentation in terms of supplying them, through an ad targeting potential cybercriminals based in France,

or international cybercriminals wanting to enter the French market.

Catch up with previous research on the topic:

- [1] Newly Launched 'Scanned Fake Passports/IDs/Credit Cards/Utility Bills' Service Randomizes and Generates

Unique Fakes On The Fly

- [2] A Peek Inside the Russian Underground Market for Fake Documents/IDs/Passports

What's so special about this underground market proposition, anyway? It's the market segmentation taking place

through the eyes of the vendor, as well as the diversity of scanned .PSD Photoshop templates, the non-modifiable

scanned documents, and the actual availability of physical fake IDs, all of them exclusively targeting the French

market segment.

Sample screenshot of the advertisement:

378



There are several types of vendors contributing to the currently mature state of the market for fake IDs/documents, or to the cybercrime ecosystem in general. Let's discuss the most popular types of market players.

Among the rarest type of such vendors is the experienced one who tends not to advertise at public or com-

mercially accessible cybercrime-friendly communities. Although it would seem fairly logical to assume that the

applied OPSEC (Operational Security) would be directly proportional with the decrease in processed orders since it

would limit the visibility of his services within the cybercrime ecosystem, that's not necessarily the case when quality,

experience, sophisticated, and, of course, high profit margins based on perceived value come into play. In between

the lack of mass advertisements, the vendor would also not list his contact details, and would only do business with cy-

bercriminals with proven reputation within not just the community in question, but also, across the entire ecosystem.

Next are those vendors who'd sacrifice OPSEC, for the sake of reaching as many customers as possible in an

attempt to monetize this market 'touch point' with other prospective cybercriminals. They advertise on public

and on commercially accessible cybercrime-friendly communities, usually have a decent reputation, with generally

positive feedback from their customers, and of course, never fail to 'deliver' what they pitch.

379

There's yet another type of such vendors, worth discussing. It's those who 'populate' a newly launched community with their propositions, and most often target novice cybercriminals with zero understanding of cybercrime

ecosystem reputation dynamics, who are still looking to purchase this desired, but largely commoditized underground

market good.

With more vendors of fake IDs/documents popping up across the entire ecosystem, the series of blog posts

profiling their activities, are prone to expand.

1. <http://ddanchev.blogspot.com/2013/07/newly-launched-scanned-fake.html>

2. <http://ddanchev.blogspot.com/2013/05/a-peek-inside-russian-underground.html>

380



The Cost of Anonymizing a Cybercriminal's Internet Activities - Part Four (2013-08-23 17:16)

Continuing the " *The Cost of Anonymizing a Cybercriminal's Internet Activities*" series, in this post, I'll profile an API-supporting, blackhat SEO-friendly vendor of anonymization services, which is currently offering hundreds of

thousands of compromised SSH accounts, HTTP/HTTPS based (compromised) proxies, and the ubiquitous for the cybercrime ecosystem, Socks 4/5 servers.

Catch up with related research on the topic:

- [1]The Cost of Anonymizing a Cybercriminal's Internet Activities - Part Three
- [2]The Cost of Anonymizing a Cybercriminal's Internet Activities
- [3]The Cost of Anonymizing a Cybercriminal's Internet Activities - Part Two
- [4]Cybercriminals SQL Inject Cybercrime-friendly Proxies Service
- [5]Malware Infected Hosts as Stepping Stones
- [6]Hacked PCs as 'anonymization stepping-stones' service operates in the open since 2004
- [7]'Malware-infected hosts as stepping stones' service offers access to hundreds of compromised U.S based hosts

- [8]New service converts malware-infected hosts into anonymization proxies

The service is currently offering access to **180,331 compromised SSH accounts, 9597 HTTP/HTTPS proxies, and**

110,185 (compromised) Socks servers located virtually all over the World.

How are they gaining access to this accounting data in the first place? Despite the overall availability of brute-

forcing tools, in 2013, one of the most popular tactic for obtaining stolen/compromised accounting data, remains the

practice of 'data mining' a botnet's already infected 'population' for virtually anything kind of accounting data, to be

later on monetized through multiple distribution/abuse channels.

Sample screenshots of the anonymization service:

381



382



Sample screenshots of the API in action:

383



384



385

What's also worth emphasizing on is the fact, that, the service is not just targeting potential cybercriminals wanting to anonymize their Internet activities, but also, [9]**black hat SEO monetizers**, who now have access to hundreds of

thousands of fresh Socks servers for the purpose of abusing them on their way to monetize their fraudulent/malicious campaigns.

[10]**Vertical market integration**, or the one-stop-shop market model, has always been an inseparable part of

the cybercrime ecosystem, as it increases the probability that a cybercriminal's one-stop-shop would immediately

occupy a larger market share within the cybercrime ecosystem, consequently resulting in more revenue from the facilitation of fraudulent and malicious activity.

Some of the most popular instances of this trendy business concept applied by cybercriminals internationally,

include but are not limited to the following real-life underground market propositions:

- A vendor of [11]**mobile spamming services** would not only offer the actual spamming process, but also, of-

fer harvested mobile mobile numbers as a value-added service, next to the on demand harvesting of mobile numbers for any given geographical region.

- A vendor of [12]**managed spam services**, would also offer the option to buy segmented and geolocated, as well

as often validated, email addresses, with the ability to perform custom harvesting for any given country

- A [13]**vendor of managed iFraming platform** would also offer access to hijacked traffic to be automatically

converted to malware-infected hosts through the platform, with additional services including as for instance,

managed crypting of the iFrame/malicious script in real-time

- An [14]**author of Web malware exploitation kit**, would be also offering managed iFrame/script crypting services

next to bulletproof hosting in case the customer desires those

The cost of anonymizing a cybercriminal's Internet activities in this particular case? The price is shaped based on the

anonymization method of choice.

This post has been reproduced from [15]Dancho Danchev's blog. Follow him [16]on Twitter.

1. <http://ddanchev.blogspot.com/2013/08/the-cost-of-anonymizing-cybercriminals.html>
2. <http://ddanchev.blogspot.com/2008/10/cost-of-anonymizing-cybercriminals.html>
3. <http://ddanchev.blogspot.com/2009/02/cost-of-anonymizing-cybercriminals.html>
4. <http://ddanchev.blogspot.com/2010/07/cybercriminals-sql-inject-cybercrime.html>
5. <http://ddanchev.blogspot.com/2008/02/malware-infected-hosts-as-stepping.html>
6. <http://blog.webroot.com/2013/03/20/hacked-pcs-as-anonymization-stepping-stones-service-operates-in-the-open-since-2004/>
7. <http://blog.webroot.com/2013/08/02/malware-infected-hosts-as-stepping-stones-service-offers-access-to-hundreds-of-compromised-u-s-based-hosts/>
8. <http://blog.webroot.com/2012/03/02/new-service-converts-malware-infected-hosts-into-anonymization-proxies/>
9. <http://ddanchev.blogspot.com/2013/04/whats-roi-on-going-to-virtual-blackhat.html>
10. <http://blog.webroot.com/2013/01/08/black-hole-exploit-kit-authors-vertical-market-integration-fuels-growth-in-malicious-web-activity/>

11. <http://blog.webroot.com/2012/05/07/managed-sms-spamming-services-going-mainstream/>
12. <http://blog.webroot.com/2012/05/17/a-peek-inside-a-managed-spam-service/>
13. <http://blog.webroot.com/2013/06/03/compromised-ftpssh-account-privilege-escalating-mass-iframe-embedding-platform-released-on-the-underground-marketplace/>

386

14. <http://blog.webroot.com/2013/01/08/black-hole-exploit-kit-authors-vertical-market-integration-fuels-growth-in-malicious-web-activity/>

15. <http://ddanchev.blogspot.com/>

16. <http://twitter.com/danchodanchev>

387

Cybercriminals Offer High Quality Plastic U.S Driving Licenses/University ID Cards (2013-08-29 02:26)

Continuing the series of blog posts profiling the most recent underground market propositions for high quality fake

passports/IDs/documents, in this post, I'll emphasize on a cybercrime-friendly vendor that's exclusively targeting the

U.S market.

Go through previous research into the market for fake passports/IDs/documents:

- [1] Newly Launched 'Scanned Fake Passports/IDs/Credit Cards/Utility Bills' Service Randomizes and Generates

Unique Fakes On The Fly

- [2] A Peek Inside the Russian Underground Market for Fake Documents/IDs/Passports
- [3] Vendor of Scanned Fake IDs, Credit Cards and Utility Bills Targets the French Market Segment

Offering fake plastic driving licenses for over 25+ U.S States, including student IDs for major U.S Universities for a static price of \$150, the vendor not just currently outperforms competing vendors in terms of quality in this particular market segment – within the cybercrime-friendly community in question – but also, is already receiving recommendations

from other cybercriminals to raise the price of his underground market 'asset', indicating penetration pricing in action.

Payment methods accepted? Bitcoin, Western Union and Moneygram.

Sample underground market ad:

[VENDOR's NAME REDACTED] has over 25+ states on tap, along with 'secondaries' to offer, all of of which and are

high quality, meaning in-state without issue, in most cases. All IDs contain UV (where applicable as some states don't), multispec-hologram, 1D/2D barcode and/or magstripe that will scan/swipe to read DMV/AAMVA license standard.

The vendor is requiring the following data from his potential customers:

Name - First, MI, Last

Address

DOB

Sex

Hair Color

Height

Weight

Eye color

Driver License number - if a number isn't provided one will be randomly generated

Endorsements and/or Restrictions - if not included these will be left blank

Scanned signature - if not provided you will receive a generic font signature

******More\Less info may be required depending on the state requested*

Scanned passport picture - no webcam pictures can be accepted.

If you cannot get a real passport picture and have a decent camera, please take a pic from the chest up against a

white background/drywall with the flash 'ON'. I will handle the cropping aspect. Also try to have good lighting and

when scanning use high resolution. You may also upload a signature. I ask that this be written using a black sharpie

style pen to achieve the best results.

388



You may upload this info to sendspace.com or the file-sharing site of your choosing and forward me the down-

load link. I will confirm reception via email and your order will begin processing. All IDs are 150USD with incentive

to group buys. Payment can be made via BTC, WU, Moneygram. Payment will be collected upon completion and approval of your order.

Sample screenshots of the service's current 'inventory':

389



390



391



392



393



394



395



396



397



398



399



400



401



402



403



404



405



406



407



408



409



410



411



412



413



414



415



416



417



418



419



420



421



422



423



424



425



426



427



428



429



430



431



432



433



434



435



436



437



438



439



440



441



442



443



444



445



446



447



448



449



450



451



452



453



454



455



456



457



458



459



460



461



462



463



464



465



466



467



468



469



470



471



472



473



474



475



476



477



478



479



480



481



482



483



484



485



486



487



488



489



490



491



492



493



494



495



496



497



498



499



500



501



502



503



504



505



506



507



508



509



510



511



512



513



514



515



516



The market for fake passports/IDs/documents is prone to flourish, as more cybercriminals demand both, scanned, and plastic fake IDs to be later one abused in related fraudulent schemes. Naturally, the market is quick to supply, and

those who excel in their Operational Security and quality of the underground market 'assets', will begin occupying a decent market share within this underground market segment.

This post has been reproduced from [4]Dancho Danchev's blog. Follow him [5]on Twitter.

1. <http://ddanchev.blogspot.com/2013/07/newly-launched-scanned-fake.html>
2. <http://ddanchev.blogspot.com/2013/05/a-peek-inside-russian-underground.html>
3. <http://ddanchev.blogspot.com/2013/08/vendor-of-scanned-fake-ids-credit-cards.html>

4. <http://ddanchev.blogspot.com/>

5. <http://twitter.com/danchodanchev>

517

Cybercriminals Offer High Quality Plastic U.S Driving Licenses/University ID Cards (2013-08-29 02:26)

Continuing the series of blog posts profiling the most recent underground market propositions for high quality fake

passports/IDs/documents, in this post, I'll emphasize on a cybercrime-friendly vendor that's exclusively targeting the

U.S market.

Go through previous research into the market for fake passports/IDs/documents:

- [1] Newly Launched 'Scanned Fake Passports/IDs/Credit Cards/Utility Bills' Service Randomizes and Generates

Unique Fakes On The Fly

- [2] A Peek Inside the Russian Underground Market for Fake Documents/IDs/Passports

- [3] Vendor of Scanned Fake IDs, Credit Cards and Utility Bills Targets the French Market Segment

Offering fake plastic driving licenses for over 25+ U.S States, including student IDs for major U.S Universities for a static price of \$150, the vendor not just currently outperforms competing vendors in terms of quality in this particular market segment – within the cybercrime-friendly community in question – but also, is already receiving recommendations

from other cybercriminals to raise the price of his underground market 'asset', indicating penetration pricing in action.

Payment methods accepted? Bitcoin, Western Union and Moneygram.

Sample underground market ad:

[VENDOR's NAME REDACTED] has over 25+ states on tap, along with 'secondaries' to offer, all of of which and are high quality, meaning in-state without issue, in most cases. All IDs contain UV (where applicable as some states don't), multispec-hologram, 1D/2D barcode and/or magstripe that will scan/swipe to read DMV/AAMVA license standard.

The vendor is requiring the following data from his potential customers:

Name - First, MI, Last

Address

DOB

Sex

Hair Color

Height

Weight

Eye color

Driver License number - if a number isn't provided one will be randomly generated

Endorsements and/or Restrictions - if not included these will be left blank

Scanned signature - if not provided you will receive a generic font signature

******More\Less info may be required depending on the state requested*

Scanned passport picture - no webcam pictures can be accepted.

If you cannot get a real passport picture and have a decent camera, please take a pic from the chest up against a

white background/drywall with the flash 'ON'. I will handle the cropping aspect. Also try to have good lighting and

when scanning use high resolution. You may also upload a signature. I ask that this be written using a black sharpie

style pen to achieve the best results.

518



You may upload this info to sendspace.com or the file-sharing site of your choosing and forward me the down-

load link. I will confirm reception via email and your order will begin processing. All IDs are 150USD with incentive

to group buys. Payment can be made via BTC, WU, Moneygram. Payment will be collected upon completion and approval of your order.

Sample screenshots of the service's current 'inventory':

519



520



521



522



523



524



525



526



527



528



529



530



531



532



533



534



535



536



537



538



539



540



541



542



543



544



545



546



547



548



549



550



551



552



553



554



555



556



557



558



559



560



561



562



563



564



565



566



567



568



569



570



571



572



573



574



575



576



577



578



579



580



581



582



583



584



585



586



587



588



589



590



591



592



593



594



595



596



597



598



599



600



601



602



603



604



605



606



607



608



609



610



611



612



613



614



615



616



617



618



619



620



621



622



623



624



625



626



627



628



629



630



631



632



633



634



635



636



637



638



639



640



641



642



643



644



645



646



The market for fake passports/IDs/documents is prone to flourish, as more cybercriminals demand both, scanned,

and plastic fake IDs to be later one abused in related fraudulent schemes. Naturally, the market is quick to supply, and

those who excel in their Operational Security and quality of the underground market 'assets', will begin occupying a

decent market share within this underground market segment.

1. <http://ddanchev.blogspot.com/2013/07/newly-launched-scanned-fake.html>
2. <http://ddanchev.blogspot.com/2013/05/a-peek-inside-russian-underground.html>
3. <http://ddanchev.blogspot.com/2013/08/vendor-of-scanned-fake-ids-credit-cards.html>

647

Profiling a Novel, High Profit Margins Oriented, Legitimate Companies Brand-Jacking Money Mule Recruitment Scheme (2013-08-29 22:41)

Over the years, I've been actively researching the money mule recruitment epidemic, providing actionable (real-

time/historical) intelligence on their activities, exposing [1]**their DNS infrastructure**, offering exclusive peek inside

[2]**the Administration Panels utilized by money mules**, emphasizing on current and emerging tactics applied by the

individuals orchestrating the final stages of a fraudulent operation - the cash out process through basic risk-forwarding.

Catch up with previous research on the money mule recruitment problem:

- [3]Spotted: cybercriminals working on new Western Union based 'money mule management' script
- [4]Keeping Money Mule Recruiters on a Short Leash - Part Eleven
- [5]Keeping Money Mule Recruiters on a Short Leash - Part Ten
- [6]Keeping Money Mule Recruiters on a Short Leash - Part Nine
- [7]Keeping Money Mule Recruiters on a Short Leash - Part Eight - Historical OSINT
- [8]Keeping Money Mule Recruiters on a Short Leash - Part Seven
- [9]Keeping Money Mule Recruiters on a Short Leash - Part Six
- [10]Keeping Money Mule Recruiters on a Short Leash - Part Five
- [11]The DNS Infrastructure of the Money Mule Recruitment Ecosystem
- [12]Keeping Money Mule Recruiters on a Short Leash - Part Four
- [13]Money Mule Recruitment Campaign Serving Client-Side Exploits
- [14]Keeping Money Mule Recruiters on a Short Leash - Part Three
- [15]Money Mule Recruiters on Yahoo!'s Web Hosting

- [16]Dissecting an Ongoing Money Mule Recruitment Campaign
- [17]Keeping Money Mule Recruiters on a Short Leash - Part Two
- [18]Keeping Reshipping Mule Recruiters on a Short Leash
- [19]Keeping Money Mule Recruiters on a Short Leash
- [20]Standardizing the Money Mule Recruitment Process
- [21]Inside a Money Laundering Group's Spamming Operations
- [22]Money Mule Recruiters use ASProx's Fast Fluxing Services
- [23]Money Mules Syndicate Actively Recruiting Since 2002

648

In this post, I'll profile a novel money mule recruitment scheme, that involves high profit margins – of course for the ones organizing the scheme – through a direct, and most importantly, (pseudo) legal brand-jacking of a

gullible business owner's brand name, enticing him/her into opening a merchant account for processing E-commerce

transactions, coming from more gullible and socially engineered mules.

It all begins with an email coming from a non-existent "environmental enterprise", that in this particular case

is abusing Google's brand in an attempt to increase the probability of a successful interaction with the socially

engineered business owners:

Sample email:

Environmental enterprise searching for representation internationally

5 % commission on 200K cash flow originated from promotion and sales of proprietary research articles

Necessary conditions:

- Own a company - Be reachable on daily basis through E-mail, phone or Skype - Proper execution of all planned

undertakings

In case if being interested, please provide:

- Name and Surname - Age - Telephone number (including country code) - City and Country - Email

Please answer to: NAME@googleapp-consult.com

Faithfully yours,

HR dept

Those who reply are kindly asked to open a merchant bank account using their own company data, and assured that,

despite the fact that the Web site which will be selling the bogus 'research articles' will be using their (legitimate)

business brand's name and contact details, they will still receive their 5 % commission on a 200,000/250,000 EUR

in anticipated revenue, which would naturally be coming directly from other mules participating in the fraudulent

scheme. Moreover, despite that a business owner will have his company brand, logo, contact information listed at

the Web site, he/she will have zero visibility to the non-existent purchasing process of this research, as " *all customer service, sales, technical logistics, etc. are to be handled by us.* "

Why would a potential cybercrime syndicate want a socially engineered business owner to open a merchant

bank account using his/her own data? Pretty simple. In my previous research on [24]**the standardization of the**

money mule recruitment process, I emphasized on how money mules are often vetted through online-based surveys,

which always ask important from a mule recruiter's perspective question, such as - when did you you first open your

bank account, and do you have any limitations on incoming/ongoing monetary transactions on it?

However, an established company would always benefit from the trust it has already established with its fi-

nancial institution/service of choice, meaning that, it will not only get its merchant account open, but also, will

successfully pass the majority of verification protection mechanisms for high volume transactions put into the place by the financial institution/service in place.

Sample reply email:

Thank you for your reply.

We are a company involved in development, branding and launching of several web media and IT projects in-

involved in consulting on green technology, renewables and alternative energy sources. Several of the projects are

being currently launched online and each one will need to have a card payment interface. This collaboration refers to

649

opening a merchant account for online credit card acceptance (E-commerce).

We would need your company to open a merchant account for card acceptance and handle the receivables

derived from the sales generated by each project. A bank/payment provider will facilitate data needed for website integration with their E-commerce payment gateway. We will handle the technical side of such integration in full.

We will brand the website under your company, therefore the administrative company data listed on the

website will be yours, but all customer service, technical logistics and sales are to be handled by us.

The products sold will be proprietary research articles and information packages on green technology, renewables and alternative

energy sources.

Incoming proceedings from sales will be settled by the bank (or the payment provider) into your business bank

account on a time scale defined by the bank (or the payment provider).

*These sale proceedings will be transferred to us, minus your commission and expenses incurred. **The volume of***

monthly payments processed through the merchant account will be in the order of EUR 200,000 - EUR 250,000 per

month in the initial months. The expected rise is roughly 5-6 % every month. The commission proposed to you

stands at 5 % of the mentioned volume.

All the expenses related to the operation including the banking and transactions fees and the merchant ac-

count setup and related fees are to be covered by us. If you agree in principle, I will provide the contract draft to

define the legal terms of our collaboration.

Yours sincerely,

Michael Torti

General Manager

ECOFIN Projects (Gibraltar)

Tel/Fax: +350 2006 1287

Who are ECOFIN Projects (**ecofinservices.net - 50.63.220.106**) ? Nothing more than [25]**a cybercrime-friendly**

"marketing agency" at its best.

650



651



652



653



654



Sample About Us description:

Ecofin is offering outstanding solutions which are useful in maximizing revenues that are generated through a wide

range of investment sectors and global assets. A wide range of services and financial opportunities are being offered

for manufacturers, developers, owners as well as financial investors interested in our niche investment portfolios and services.

We are operating as a globally safe company as well as involving risk and integrity management expertise

that brings together practical experience along with cutting edge, innovative engineering and technologies. The

company is research based which is primarily focused on environmental sectors, alternative energy, infrastructure, as well as utility all around the globe.

The firm is practicing a fundamental and basic approach while it comes to managing its clientele assets. Ecofin is

useful in developing, branding as well as launching exclusive information sales podiums based on alternative, as well

as green technological sources along with IT and web media themes. The company is dedicated to providing its clients

with the highest levels of quality services and investment returns within the niche industries that we focus upon.

655



Contact details:

+350 200 67911 (Gibraltar)

+852 5808 2461 (Hong Kong)

+54 11 5984 1154 (Buenos Aires)

+44 20 3051 6249 (London)

Skype: ecofin2013

Suite 4, 209 Main Street

Gibraltar GBZ 1AA

A potentially socially engineered business owner would then be contacted with a similar email:

Please find the Contract draft attached, review and confirm your agreement with every point of it. The next step

would be to provide the proper company data to be put in the contract and produce the final version for the signing.

Please review the showcase website:

This site will be copied into a new domain reflecting your company name and your company data.

As indicated, all customer service, sales, technical logistics, etc. are to be handled by us. You would need to open a merchant account for online credit card acceptance (E-commerce).

The customers will be from all over the world. All the issues related to sales, marketing, customer service, sup-

ply, logistics, etc. are to be handled by us. You will be required to open a merchant account for online credit card

acceptance, receive the funds and transfer us the proceedings, as indicated in the contract draft with detail.

No

capital or any upfront payments from your side are required. If it is necessary to cover any upfront fees for the merchant account establishment, we will transfer such fees to you beforehand.

Sample Web Site Template offered as an example of how a socially engineered business owner's company

branded Web site, would look like (**greentechidea.com - 50.63.39.1**):

656



657



658



Sample copy of the Contract:

659



660



661



662



663



664



Sample domains from the mule recruitment campaigns spamvertised over email:

googleapp-consult.com

googleapps-euro.com

worlds-trade.com

trades-consult.com

worlds-diploms.com

Sample name servers involved in the campaign:

NS1.ELCACAREO.NET - 184.82.62.16; 136.0.16.169;
184.82.204.70 - Email: shanghaiherald32@yahoo.com

NS2.ELCACAREO.NET - 6.87.78.121

The same email (shanghaiherald32@yahoo.com) is also known to have also been used to register the fol-

lowing fraudulent/malicious domains:

badstylecorps.com

tvblips.net

viperlair.net

[26]"The only green is money".

This post has been reproduced from [27]Dancho Danchev's blog. Follow him [28]on Twitter.

1. <http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html>
2. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>
3. <http://blog.webroot.com/2013/03/22/spotted-cybercriminals-working-on-new-western-union-based-money-mule-management-script/>
4. <http://ddanchev.blogspot.com/2011/08/keeping-money-mule-recruiters-on-short.html>
5. <http://ddanchev.blogspot.com/2011/07/keeping-money-mule-recruiters-on-short.html>
6. http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short_30.html
7. http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short_25.html
8. <http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short.html>
9. <http://ddanchev.blogspot.com/2011/03/keeping-money-mule-recruiters-on-short.html>
10. <http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html>

11. <http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html>
12. <http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html>
13. <http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html>
14. <http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html>
15. <http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html>
16. <http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html>
17. <http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html>
18. <http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html>
19. <http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html>
20. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>
21. <http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html>
22. <http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asprox-fast.html>

23. <http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html>
24. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>
25. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>
26. <http://www.imdb.com/title/tt1027718>
27. <http://ddanchev.blogspot.com/>
28. <http://twitter.com/danchodanchev>

666

Profiling a Novel, High Profit Margins Oriented, Legitimate Companies Brand-Jacking Money Mule Recruitment Scheme (2013-08-29 22:41)

Over the years, I've been actively researching the money mule recruitment epidemic, providing actionable (real-time/historical) intelligence on their activities, exposing [1]**their DNS infrastructure**, offering exclusive peek inside

[2]**the Administration Panels utilized by money mules**, emphasizing on current and emerging tactics applied by the

individuals orchestrating the final stages of a fraudulent operation - the cash out process through basic risk-forwarding.

Catch up with previous research on the money mule recruitment problem:

- [3]Spotted: cybercriminals working on new Western Union based 'money mule management' script
- [4]Keeping Money Mule Recruiters on a Short Leash - Part Eleven
- [5]Keeping Money Mule Recruiters on a Short Leash - Part Ten
- [6]Keeping Money Mule Recruiters on a Short Leash - Part Nine
- [7]Keeping Money Mule Recruiters on a Short Leash - Part Eight - Historical OSINT
- [8]Keeping Money Mule Recruiters on a Short Leash - Part Seven
- [9]Keeping Money Mule Recruiters on a Short Leash - Part Six
- [10]Keeping Money Mule Recruiters on a Short Leash - Part Five
- [11]The DNS Infrastructure of the Money Mule Recruitment Ecosystem
- [12]Keeping Money Mule Recruiters on a Short Leash - Part Four
- [13]Money Mule Recruitment Campaign Serving Client-Side Exploits
- [14]Keeping Money Mule Recruiters on a Short Leash - Part Three

- [15]Money Mule Recruiters on Yahoo!'s Web Hosting
- [16]Dissecting an Ongoing Money Mule Recruitment Campaign
- [17]Keeping Money Mule Recruiters on a Short Leash - Part Two
- [18]Keeping Reshipping Mule Recruiters on a Short Leash
- [19]Keeping Money Mule Recruiters on a Short Leash
- [20]Standardizing the Money Mule Recruitment Process
- [21]Inside a Money Laundering Group's Spamming Operations
- [22]Money Mule Recruiters use ASProx's Fast Fluxing Services
- [23]Money Mules Syndicate Actively Recruiting Since 2002

667

In this post, I'll profile a novel money mule recruitment scheme, that involves high profit margins – of course for the ones organizing the scheme – through a direct, and most importantly, (pseudo) legal brand-jacking of a

gullible business owner's brand name, enticing him/her into opening a merchant account for processing E-commerce

transactions, coming from more gullible and socially engineered mules.

It all begins with an email coming from a non-existent "environmental enterprise", that in this particular case

is abusing Google's brand in an attempt to increase the probability of a successful interaction with the socially

engineered business owners:

Sample email:

Environmental enterprise searching for representation internationally

5 % commission on 200K cash flow originated from promotion and sales of proprietary research articles

Necessary conditions:

- Own a company - Be reachable on daily basis through E-mail, phone or Skype - Proper execution of all planned

undertakings

In case if being interested, please provide:

- Name and Surname - Age - Telephone number (including country code) - City and Country - Email

Please answer to: NAME@googleapp-consult.com

Faithfully yours,

HR dept

Those who reply are kindly asked to open a merchant bank account using their own company data, and assured that,

despite the fact that the Web site which will be selling the bogus 'research articles' will be using their (legitimate)

business brand's name and contact details, they will still receive their 5 % commission on a 200,000/250,000 EUR

in anticipated revenue, which would naturally be coming directly from other mules participating in the fraudulent

scheme. Moreover, despite that a business owner will have his company brand, logo, contact information listed at

the Web site, he/she will have zero visibility to the non-existent purchasing process of this research, as " *all customer service, sales, technical logistics, etc. are to be handled by us.* "

Why would a potential cybercrime syndicate want a socially engineered business owner to open a merchant

bank account using his/her own data? Pretty simple. In my previous research on [24]**the standardization of the**

money mule recruitment process, I emphasized on how money mules are often vetted through online-based surveys,

which always ask important from a mule recruiter's perspective question, such as - when did you you first open your

bank account, and do you have any limitations on incoming/ongoing monetary transactions on it?

However, an established company would always benefit from the trust it has already established with its fi-

nancial institution/service of choice, meaning that, it will not only get its merchant account open, but also, will

successfully pass the majority of verification protection mechanisms for high volume transactions put into the place by the financial institution/service in place.

Sample reply email:

Thank you for your reply.

We are a company involved in development, branding and launching of several web media and IT projects in-

involved in consulting on green technology, renewables and alternative energy sources. Several of the projects are

being currently launched online and each one will need to have a card payment interface. This collaboration refers to

668

opening a merchant account for online credit card acceptance (E-commerce).

We would need your company to open a merchant account for card acceptance and handle the receivables

derived from the sales generated by each project. A bank/payment provider will facilitate data needed for website integration with their E-commerce payment gateway. We will handle the technical side of such integration in full.

We will brand the website under your company, therefore the administrative company data listed on the

website will be yours, but all customer service, technical logistics and sales are to be handled by us.

The products sold will be proprietary research articles and information packages on green technology, renewables and alternative

energy sources.

Incoming proceedings from sales will be settled by the bank (or the payment provider) into your business bank

account on a time scale defined by the bank (or the payment provider).

*These sale proceedings will be transferred to us, minus your commission and expenses incurred. **The volume of***

monthly payments processed through the merchant account will be in the order of EUR 200,000 - EUR 250,000 per

month in the initial months. The expected rise is roughly 5-6 % every month. The commission proposed to you

stands at 5 % of the mentioned volume.

All the expenses related to the operation including the banking and transactions fees and the merchant ac-

count setup and related fees are to be covered by us. If you agree in principle, I will provide the contract draft to

define the legal terms of our collaboration.

Yours sincerely,

Michael Torti

General Manager

ECOFIN Projects (Gibraltar)

Tel/Fax: +350 2006 1287

Who are ECOFIN Projects (**ecofinservices.net - 50.63.220.106**) ? Nothing more than [25]a **cybercrime-friendly**

"marketing agency" at its best.

669



670



671



672



673



Sample About Us description:

Ecofin is offering outstanding solutions which are useful in maximizing revenues that are generated through a wide

range of investment sectors and global assets. A wide range of services and financial opportunities are being offered

for manufacturers, developers, owners as well as financial investors interested in our niche investment portfolios and services.

We are operating as a globally safe company as well as involving risk and integrity management expertise

that brings together practical experience along with cutting edge, innovative engineering and technologies. The

company is research based which is primarily focused on environmental sectors, alternative energy, infrastructure, as well as utility all around the globe.

The firm is practicing a fundamental and basic approach while it comes to managing its clientele assets. Ecofin is

useful in developing, branding as well as launching exclusive information sales podiums based on alternative, as well

as green technological sources along with IT and web media themes. The company is dedicated to providing its clients

with the highest levels of quality services and investment returns within the niche industries that we focus upon.

674



Contact details:

+350 200 67911 (Gibraltar)

+852 5808 2461 (Hong Kong)

+54 11 5984 1154 (Buenos Aires)

+44 20 3051 6249 (London)

Skype: ecofin2013

Suite 4, 209 Main Street

Gibraltar GBZ 1AA

A potentially socially engineered business owner would then be contacted with a similar email:

Please find the Contract draft attached, review and confirm your agreement with every point of it. The next step

would be to provide the proper company data to be put in the contract and produce the final version for the signing.

Please review the showcase website:

This site will be copied into a new domain reflecting your company name and your company data.

As indicated, all customer service, sales, technical logistics, etc. are to be handled by us. You would need to open a merchant account for online credit card acceptance (E-commerce).

The customers will be from all over the world. All the issues related to sales, marketing, customer service, sup-

ply, logistics, etc. are to be handled by us. You will be required to open a merchant account for online credit card

acceptance, receive the funds and transfer us the proceedings, as indicated in the contract draft with detail.

No

capital or any upfront payments from your side are required. If it is necessary to cover any upfront fees for the merchant account establishment, we will transfer such fees to you beforehand.

Sample Web Site Template offered as an example of how a socially engineered business owner's company

branded Web site, would look like (**greentechidea.com - 50.63.39.1**):

675



676



677



Sample copy of the Contract:

678



679



680



681



682



683



Sample domains from the mule recruitment campaigns spamvertised over email:

googleapp-consult.com

googleapps-euro.com

worlds-trade.com

trades-consult.com

worlds-diploms.com

Sample name servers involved in the campaign:

NS1.ELCACAREO.NET - 184.82.62.16; 136.0.16.169;
184.82.204.70 - Email: shanghaiherald32@yahoo.com

NS2.ELCACAREO.NET - 6.87.78.121

The same email (shanghaiherald32@yahoo.com) is also known to have also been used to register the fol-

lowing fraudulent/malicious domains:

badstylecorps.com

tvblips.net

viperlair.net

[26]"The only green is money".

This post has been reproduced from [27]Dancho Danchev's blog. Follow him [28]on Twitter.

1. <http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html>
2. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>
3. <http://blog.webroot.com/2013/03/22/spotted-cybercriminals-working-on-new-western-union-based-money-mule-management-script/>
4. <http://ddanchev.blogspot.com/2011/08/keeping-money-mule-recruiters-on-short.html>
5. <http://ddanchev.blogspot.com/2011/07/keeping-money-mule-recruiters-on-short.html>
6. http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short_30.html
7. http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short_25.html
8. <http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short.html>
9. <http://ddanchev.blogspot.com/2011/03/keeping-money-mule-recruiters-on-short.html>
10. <http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html>

11. <http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html>
12. <http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html>
13. <http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html>
14. <http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html>
15. <http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html>
16. <http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html>
17. <http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html>
18. <http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html>
19. <http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html>
20. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>
21. <http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html>
22. <http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asprox-fast.html>

23. <http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html>
24. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>
25. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>
26. <http://www.imdb.com/title/tt1027718>
27. <http://ddanchev.blogspot.com/>
28. <http://twitter.com/danchodanchev>

685



Summarizing Webroot's Threat Blog Posts for August (2013-08-30 14:11)

The following is a brief summary of all of my posts at [1]**Webroot's Threat Blog** for August, 2013. You can subscribe to [2]**Webroot's Threat Blog RSS Feed**, or follow me on Twitter:

01. [3]'Malware-infected hosts as stepping stones' service offers access to hundreds of compromised U.S based

hosts

02. [4]New 'Hacked shells as a service' empowers cybercriminals with access to high page rank-ed Web sites

03. [5]Fake 'iPhone Picture Snapshot Message' themed emails lead to malware

04. [6]Malicious Bank of America (BofA) 'Statement of Expenses' themed emails lead to client-side exploits and malware

05. [7]Cybercriminals spamvertise fake 'O2 U.K MMS' themed emails, serve malware

06. [8]One-stop-shop for spammers offers DKIM-verified SMTP servers, harvested email databases and training to potential customers

07. [9]Fake 'Apple Store Gift Card' themed emails serve client-side exploits and malware

08. [10]Newly launched managed 'malware dropping' service spotted in the wild

09. [11]Cybercrime-friendly underground traffic exchange helps facilitate fraudulent and malicious activity

10. [12]From Vietnam with tens of millions of harvested emails, spam-ready SMTP servers and DIY spamming tools

11. [13]DIY Craigslist email collecting tools empower spammers with access to fresh/valid email addresses

12. [14]Bulletproof TDS/Doorways/Pharma/Spam/Warez hosting service operates in the open since 2009

686

13. [15]DIY automatic cybercrime-friendly 'redirectors generating' service spotted in the wild

14. [16]Cybercriminals offer spam-ready SMTP servers for rent/direct managed purchase

15. [17]Cybercrime-friendly underground traffic exchanges help facilitate fraudulent and malicious activity – part

two

This post has been reproduced from [18]Dancho Danchev's blog . Follow him [19]on Twitter.

1. <http://blog.webroot.com/>

2. <http://feeds2.feedburner.com/WebrootThreatBlog>

3. <http://blog.webroot.com/2013/08/02/malware-infected-hosts-as-stepping-stones-service-offers-access-to-hundreds-of-compromised-u-s-based-hosts/>

[dreds-of-compromised-u-s-based-hosts/](http://blog.webroot.com/2013/08/02/malware-infected-hosts-as-stepping-stones-service-offers-access-to-hundreds-of-compromised-u-s-based-hosts/)

4.

<http://blog.webroot.com/2013/08/02/new-hacked-shells-as-a-service-empowers-cybercriminals-with-access-to-high-page-rank-ed-web-sites/>

[high-page-rank-ed-web-sites/](http://blog.webroot.com/2013/08/02/new-hacked-shells-as-a-service-empowers-cybercriminals-with-access-to-high-page-rank-ed-web-sites/)

5. <http://blog.webroot.com/2013/08/05/fake-iphone-picture-snapshot-message-themed-emails-lead-to-malware/>

6. <http://blog.webroot.com/2013/08/06/malicious-bank-of-america-bofa-statement-of-expenses-themed-emails-lead-to-client-side-exploits-and-malware/>

[d-to-client-side-exploits-and-malware/](http://blog.webroot.com/2013/08/06/malicious-bank-of-america-bofa-statement-of-expenses-themed-emails-lead-to-client-side-exploits-and-malware/)

7. <http://blog.webroot.com/2013/08/07/cybercriminals-spamvertise-fake-o2-u-k-mms-themed-emails-serve-malware/>

/

8. <http://blog.webroot.com/2013/08/08/one-stop-shop-for-spammers-offers-dkim-verified-smtp-servers-harvested-email-databases-and-training-to-potential-customers/>

9. <http://blog.webroot.com/2013/08/09/fake-apple-store-gift-card-themed-emails-serve-client-side-exploits-and-malware/>

10. <http://blog.webroot.com/2013/08/12/newly-launched-managed-malware-dropping-service-spotted-in-the-wild/>

11. <http://blog.webroot.com/2013/08/13/cybercrime-friendly-underground-traffic-exchange-helps-facilitate-fraudulent-and-malicious-activity/>

12.

<http://blog.webroot.com/2013/08/14/from-vietnam-with-tens-of-millions-of-harvested-emails-spam-ready-smtp-servers-and-diy-spamming-tools/>

13. <http://blog.webroot.com/2013/08/15/diy-craigslist-email-collecting-tools-empower-spammers-with-access-to-fresh-valid-email-addresses/>

14. <http://blog.webroot.com/2013/08/16/bulletproof-tdsdoorwayspharmaspamwarez-hosting-service-operates-in-the-us-open-since-2009/>

15. <http://blog.webroot.com/2013/08/19/diy-automatic-cybercrime-friendly-redirectors-generating-service-spott>

[ed-in-the-wild/](#)

16. <http://blog.webroot.com/2013/08/28/cybercriminals-offer-spam-ready-smtp-servers-for-rentdirect-managed-purchase/>

17. <http://blog.webroot.com/2013/08/29/cybercrime-friendly-underground-traffic-exchanges-help-facilitate-fraudulent-and-malicious-activity-part-two/>

18. <http://ddanchev.blogspot.com/>

19. <http://twitter.com/danchodanchev>

687

1.9

September

688



Rogue iFrame Injected Web Sites Lead to the AndroidOS/FakeInst/Trojan-SMS.J2ME.JiFake Mobile Mal-

ware (2013-09-16 14:29)

A currently ongoing malicious campaign relying on injected iFrames at legitimate Web sites, successfully [1]**segments**

mobile traffic, and exposes mobile users to fraudulent legitimately looking variants of the AndroidOS/FakeInst/TrojanSMS.J2ME.JiFake mobile malware.

Let's dissect the campaign, expose the domains portfolio currently/historically known to have been involved

in this campaign, as well as list all the malicious MD5s known to have been pushed by it.

iFrame injected domains containing the mobile traffic segmentation script parked on the same IP:

asphalt7-android.org - 93.170.109.193

fifa12-android.org

gta3-android.org

fruit-ninja-android.org

wildblood-android.org

osmos-android.org

moderncombat-android.org

minecraft-android.org

googlanalytics.ws

getinternet.ws

ddlloads.com

googlecount.ws

opera-com.com

opgrade.ws

statuses.ws

ya-googl.ws

yadirect.ws

yandex-google.ws

689



Sample mobile malware MD5s pushed by the campaign:

[2]MD5: e77f3bffe18fb9f5a1b1e5e6a0b8aaf8

[3]

MD5: 5fb4cc0b0d8dfe8011c44f97c6dd0aa2[4]

[5]

MD5: 9348b5a13278cc101ae95cb2a88fe403[6]

[7]MD5: f4966c315dafa7e39ad78e31e599e8d0

[8]MD5: 6f839dd29d2c7807043d06ba19e9c916

[9]MD5: 8cfefba7175e6e9a10e2a9ade4d87405

[10]MD5: 4e5af55dd6a310bced83eb08c9a635b3

Phone back location:

*hxxp://depositmobi.com/getTask.php/task=updateOpening
&s= - 93.170.107.130*

Parked on the same IP (93.170.107.130) are also the following domains participating in the campaign's infrastructure:

123diskapp.com

1gameminecraft.ru

2010mobile.ru

absex.ru

690

ammla.info

and4mobiles.ru

android-apk-file.ru

android-games-skachat.ru.com

android-key.ru

android-market-apk.ru

android-market-cools.ru

android-vk.com

android7s.ru

androidcool.tk

androiderus.com

androidnns.ru

androidone.net

androidperfomance.com

androids-market.ru

androidupos.ru

24-android.ru

online-android.ru

moiandroid.ru

ktozdesj.ru

super-androids.ru

The following malicious mobile malware MD5s are known to have phoned back to the same IP in the past:

[11]MD5: 572b07bd031649d4a82bb392156b25c6

[12]MD5: 9685ff439e610fa8f874bf216fa47eee

[13]MD5: 6d9dd3c9671d3d88f16071f1483faa12

[14]MD5: 276b77b3242cb0f767bfba0009bcf3e7

[15]MD5: aefdbdee7f873441b9d53500e1af34fa

What's also worth emphasizing on is that we've also got a decent number of malicious Windows samples

known to have phoned back to the same IP in the past, presumably in an attempt by fellow cybercriminals to

monetize the traffic through an affiliate program.

MD5: bac8f2c5d0583ee8477d79dc52414bf5

MD5: a1ae35eadf7599d2f661a9ca7f0f2150

MD5: 419fdb78356eaf61f9445cf828b3e5cf

MD5: abce96eaa7c345c2c3a89a8307524001

MD5: 93d11dc11cccc5ac5a1d57edce73ea07

MD5: 53bbad9018cd53d16fb1a21bd4738619

MD5: 15f3eca26f6c8d12969ffb1dbeead236

MD5: 72c6c14f9bab8ff95dbaf491f2a2aff6

MD5: a282b40d654fee59a586b89a1a12cac2

MD5: e0798c635d263f15ab54a839bf6bac7f

MD5: 7b1d8820cc012deac282fc72471310bd

MD5: 21fdbb9e9e13297ae12768764e169fb4

MD5: 47fa4a3a7d94dad9fac1cbdc07862496

MD5: 5e9321027c73175cf6ff862019c90af7

MD5: cfbaccc61dc51b805673000d09e99024

MD5: 8bc4dd1aff76fd4d2513af4538626033

MD5: f6a622f76b18d3fa431a34eb33be4619

MD5: c068d11293fc14bebdf3b3827e0006ac

691



MD5: d68338a37f62e26e701dfe45a2f9cbf2

MD5: e1c9562b6666d9915c7748c25376416f

MD5: 1dccd14b23698ecc7c5a4b9099954ae4

MD5: 47601e9f8b624464b63d499af60f6c18

Actual download location of a sample mobile malware sample:

*hxxp://mediaworks3.com/getfile.php?dtype=dle &u=getfl
&d=FLVPLayer - 78.140.131.124*

The following mobile malware serving domains are also known to have responded to the same IP (78.140.131.124)

in the past:

4apkser.ru

absex.ru

agw-railway.com

androedis.ru

android-apk-file.ru

android-update.name

android6s.ru

android7s.ru

androidappfile.name

androidaps.ru

androidbizarre.com

androidilve.ru

androidovnlloads.com

androidupss.ru

apk-load.ru

692

apkzona.ru

bali-special.ru

com-opera.com

dml-site.ru

download-opera.com

As well as the following malicious MD5s:

[16]MD5: 8cfefbfa7175e6e9a10e2a9ade4d87405

[17]MD5: 4e5af55dd6a310bced83eb08c9a635b3

Thanks to the commercial availability of [18]**DIY iFrame injecting platforms**, the current [19]**commoditization**

of hacked/compromised accounts across multiple verticals, the [20]**efficiency-oriented mass SQL injection cam-**

paings, as well as the existence of beneath the radar [21]**malvertising campaigns**, cybercriminals are perfectly positioned to continue monetizing mobile traffic for fraudulent/malicious purposes.

This post has been reproduced from [22]Dancho Danchev's blog . Follow him [23]on Twitter.

1.

<http://www.webroot.com/blog/2013/08/29/cybercrime-friendly-underground-traffic-exchanges-help-facilitate-fraudulent-and-malicious-activity-part-two/>

2.

<https://www.virustotal.com/en/file/60a67827997b60fcbbf5a625f809c7ed559475e12f36697349e6178c7036d38e/analysis/>

3. <http://draft.blogger.com/>

4. <http://draft.blogger.com/null>

5.

<https://www.virustotal.com/en/file/9262af1bbb4c392aaca2ca3ad321bd068cf37d99ed8845fe5ae2769a5a7810ec/analysis/>

6. <http://draft.blogger.com/>

7.

<https://www.virustotal.com/en/file/f5124c25f48746652a4bd345442e12b4f63d9acd7d7974addc3a3168f22e8bb5/analysis/>

8.

<https://www.virustotal.com/en/file/eb974ff155067f160f7200>

[f31ee703472bb082f7e7bf296a5e189572f2841240/analysis/](https://www.virustotal.com/en/file/f31ee703472bb082f7e7bf296a5e189572f2841240/analysis/)

9.
<https://www.virustotal.com/en/file/101edaf46ef9a1d76f9ab8a2d12ae24ca7dae0011d4ffb602e456a11305fa332/analysis/>

10.
<https://www.virustotal.com/en/file/d2e38295ba6c133c98c7d6179323d7d68b066bc5af123466e83e9352860f846a/analysis/>

11.
<https://www.virustotal.com/en/file/a4d02a98d8e4a1152b71cfde6bb897f9923f51440ba41d4263cafde7a3fadb94/analysis/>

12.
<https://www.virustotal.com/en/file/2bd3bca6a432fc5fb5f56bf6b029a7b471caf03d882fb89133b8b963e5bd5188/analysis/>

13.
<https://www.virustotal.com/en/file/1235f1fcce45696a6a5f44bcde505d7efe333978a0eb3a10a9e178cd1d2ba967/analysis/>

14.
<https://www.virustotal.com/en/file/c6de29e62fd774aee3550>

[285ed79d32d30427bb105e205806c8b885d6f33adc0/analysis/](https://www.virustotal.com/en/file/285ed79d32d30427bb105e205806c8b885d6f33adc0/analysis/)

[is/](#)

15.

<https://www.virustotal.com/en/file/72adb6e21c8001208d60cff662bcbff96133f4f1342c3d53f7e3080825fb1b60/analysis/>

[is/](#)

16.

<https://www.virustotal.com/en/file/101edaf46ef9a1d76f9ab8a2d12ae24ca7dae0011d4ffb602e456a11305fa332/analysis/>

[is/](#)

17.

<https://www.virustotal.com/en/file/d2e38295ba6c133c98c7d6179323d7d68b066bc5af123466e83e9352860f846a/analysis/>

[is/](#)

18. <http://www.webroot.com/blog/2013/06/03/compromised-ftpssh-account-privilege-escalating-mass-iframe-embedding-platform-released-on-the-underground-marketplace/>

[693](#)

693

19. <http://www.webroot.com/blog/tag/hacked-accounts/>

20. <https://www.google.com/webhp?hl=en&tab=ww#hl=en&q=site:ddanchev.blogspot.com+sql+injection>

21. <http://ddanchev.blogspot.com/2009/09/ukrainian-fan-club-features.html>

22. <http://ddanchev.blogspot.com/>

23. <http://twitter.com/danchodanchev>

694



Rogue iFrame Injected Web Sites Lead to the AndroidOS/FakeInst/Trojan-SMS.J2ME.JiFake Mobile Mal-

ware (2013-09-16 14:29)

A currently ongoing malicious campaign relying on injected iFrames at legitimate Web sites, successfully [1]**segments**

mobile traffic, and exposes mobile users to fraudulent legitimately looking variants of the AndroidOS/FakeInst/TrojanSMS.J2ME.JiFake mobile malware.

Let's dissect the campaign, expose the domains portfolio currently/historically known to have been involved

in this campaign, as well as list all the malicious MD5s known to have been pushed by it.

iFrame injected domains containing the mobile traffic segmentation script parked on the same IP:

asphalt7-android.org - 93.170.109.193

fifa12-android.org

gta3-android.org

fruit-ninja-android.org
wildblood-android.org
osmos-android.org
moderncombat-android.org
minecraft-android.org
googlanalytics.ws
getinternet.ws
ddlloads.com
googlecount.ws
opera-com.com
opgrade.ws
statuses.ws
ya-googl.ws
yadirect.ws
yandex-google.ws

695



Sample mobile malware MD5s pushed by the campaign:

[2]MD5: e77f3bffe18fb9f5a1b1e5e6a0b8aaf8

[3]

MD5: 5fb4cc0b0d8dfe8011c44f97c6dd0aa2[4]

[5]

MD5: 9348b5a13278cc101ae95cb2a88fe403[6]

[7]MD5: f4966c315dafa7e39ad78e31e599e8d0

[8]MD5: 6f839dd29d2c7807043d06ba19e9c916

[9]MD5: 8cfefbfa7175e6e9a10e2a9ade4d87405

[10]MD5: 4e5af55dd6a310bced83eb08c9a635b3

Phone back location:

*hxxp://depositmobi.com/getTask.php/task=updateOpening
&s= - 93.170.107.130*

Parked on the same IP (93.170.107.130) are also the following domains participating in the campaign's infrastructure:

123diskapp.com

1gameminecraft.ru

2010mobile.ru

absex.ru

696

ammla.info

and4mobiles.ru

android-apk-file.ru

android-games-skachat.ru.com

android-key.ru

android-market-apk.ru

android-market-cools.ru

android-vk.com

android7s.ru

androidcool.tk

androiderus.com

androidnns.ru

androidone.net

androidperfomance.com

androids-market.ru

androidupos.ru

24-android.ru

online-android.ru

moiandroid.ru

ktozdesj.ru

super-androids.ru

The following malicious mobile malware MD5s are known to have phoned back to the same IP in the past:

[11]MD5: 572b07bd031649d4a82bb392156b25c6

[12]MD5: 9685ff439e610fa8f874bf216fa47eee

[13]MD5: 6d9dd3c9671d3d88f16071f1483faa12

[14]MD5: 276b77b3242cb0f767bfba0009bcf3e7

[15]MD5: aefdbdee7f873441b9d53500e1af34fa

What's also worth emphasizing on is that we've also got a decent number of malicious Windows samples

known to have phoned back to the same IP in the past, presumably in an attempt by fellow cybercriminals to

monetize the traffic through an affiliate program.

MD5: bac8f2c5d0583ee8477d79dc52414bf5

MD5: a1ae35eadf7599d2f661a9ca7f0f2150

MD5: 419fdb78356eaf61f9445cf828b3e5cf

MD5: abce96eaa7c345c2c3a89a8307524001

MD5: 93d11dc11cccc5ac5a1d57edce73ea07

MD5: 53bbad9018cd53d16fb1a21bd4738619

MD5: 15f3eca26f6c8d12969ffb1dbeead236

MD5: 72c6c14f9bab8ff95dbaf491f2a2aff6

MD5: a282b40d654fee59a586b89a1a12cac2

MD5: e0798c635d263f15ab54a839bf6bac7f

MD5: 7b1d8820cc012deac282fc72471310bd

MD5: 21fdbb9e9e13297ae12768764e169fb4

MD5: 47fa4a3a7d94dad9fac1cbdc07862496

MD5: 5e9321027c73175cf6ff862019c90af7

MD5: cfbaccc61dc51b805673000d09e99024

MD5: 8bc4dd1aff76fd4d2513af4538626033

MD5: f6a622f76b18d3fa431a34eb33be4619

MD5: c068d11293fc14bebd3b3827e0006ac

697



MD5: d68338a37f62e26e701dfe45a2f9cbf2

MD5: e1c9562b6666d9915c7748c25376416f

MD5: 1dccd14b23698ecc7c5a4b9099954ae4

MD5: 47601e9f8b624464b63d499af60f6c18

Actual download location of a sample mobile malware sample:

*hxxp://mediaworks3.com/getfile.php?dtype=dle &u=getfl
&d=FLVPLayer - 78.140.131.124*

The following mobile malware serving domains are also known to have responded to the same IP (78.140.131.124)

in the past:

4apkser.ru

absex.ru

agw-railway.com

androedis.ru

android-apk-file.ru

android-update.name

android6s.ru

android7s.ru

androidappfile.name

androidaps.ru

androidbizarre.com

androidilve.ru

androidovnlods.com

androidupss.ru

apk-load.ru

698

apkzona.ru

bali-special.ru

com-opera.com

dml-site.ru

download-opera.com

As well as the following malicious MD5s:

[16]MD5: 8cfefbfa7175e6e9a10e2a9ade4d87405

[17]MD5: 4e5af55dd6a310bced83eb08c9a635b3

Thanks to the commercial availability of [18]**DIY iFrame injecting platforms**, the current [19]**commoditization**

of hacked/compromised accounts across multiple verticals, the [20]**efficiency-oriented mass SQL injection cam-**

paings, as well as the existence of beneath the radar [21]**malvertising campaigns**, cybercriminals are perfectly positioned to continue monetizing mobile traffic for fraudulent/malicious purposes.

Updates will be posted as soon as new developments take place.

1.

<http://www.webroot.com/blog/2013/08/29/cybercrime-friendly-underground-traffic-exchanges-help-facilitate-fraudulent-and-malicious-activity-part-two/>

2.

<https://www.virustotal.com/en/file/60a67827997b60fcbbf5a625f809c7ed559475e12f36697349e6178c7036d38e/analysis/>

3. <http://draft.blogger.com/>

4. <http://draft.blogger.com/null>

5.

<https://www.virustotal.com/en/file/9262af1bbb4c392aaca2ca3ad321bd068cf37d99ed8845fe5ae2769a5a7810ec/analysis/>

6. <http://draft.blogger.com/>

7.

<https://www.virustotal.com/en/file/f5124c25f48746652a4bd345442e12b4f63d9acd7d7974addc3a3168f22e8bb5/analysis/>

[is/](#)

8.

<https://www.virustotal.com/en/file/eb974ff155067f160f7200f31ee703472bb082f7e7bf296a5e189572f2841240/analysis/>

[is/](#)

9.

<https://www.virustotal.com/en/file/101edaf46ef9a1d76f9ab8a2d12ae24ca7dae0011d4ffb602e456a11305fa332/analysis/>

[is/](#)

10.

<https://www.virustotal.com/en/file/d2e38295ba6c133c98c7d6179323d7d68b066bc5af123466e83e9352860f846a/analysis/>

[is/](#)

11.

<https://www.virustotal.com/en/file/a4d02a98d8e4a1152b71cfde6bb897f9923f51440ba41d4263cafde7a3fadb94/analysis/>

[is/](#)

12.

<https://www.virustotal.com/en/file/2bd3bca6a432fc5fb5f56bf6b029a7b471caf03d882fb89133b8b963e5bd5188/analysis/>

[is/](#)

13.

<https://www.virustotal.com/en/file/1235f1fcce45696a6a5f44bcde505d7efe333978a0eb3a10a9e178cd1d2ba967/analysis/>

[is/](#)

14.

<https://www.virustotal.com/en/file/c6de29e62fd774aee3550285ed79d32d30427bb105e205806c8b885d6f33adc0/analysis/>

[is/](#)

15.

<https://www.virustotal.com/en/file/72adb6e21c8001208d60cff662bcbff96133f4f1342c3d53f7e3080825fb1b60/analysis/>

[is/](#)

16.

<https://www.virustotal.com/en/file/101edaf46ef9a1d76f9ab8a2d12ae24ca7dae0011d4ffb602e456a11305fa332/analysis/>

[is/](#)

17.

<https://www.virustotal.com/en/file/d2e38295ba6c133c98c7d6179323d7d68b066bc5af123466e83e9352860f846a/analysis/>

[is/](#)

18. <http://www.webroot.com/blog/2013/06/03/compromised-ftpssh-account-privilege-escalating-mass-iframe-embedd>

[699](#)

[ing-platform-released-on-the-underground-marketplace/](#)

19. <http://www.webroot.com/blog/tag/hacked-accounts/>

20. [https://www.google.com/webhp?](https://www.google.com/webhp?hl=en&tab=ww#hl=en&q=site:ddanchev.blogspot.com+sql+injection)

[hl=en&tab=ww#hl=en&q=site:ddanchev.blogspot.com+sql+injection](#)

21. <http://ddanchev.blogspot.com/2009/09/ukrainian-fan-club-features.html>

700



Dissecting FireEye's Career Web Site Compromise (2013-09-18 19:41)

Remember when back in 2010, I established a direct connection between several [1]**mass Wordpress blogs com-**

promise campaigns, with the campaign behind the [2]**compromised Web site of the U.S. Treasury**, prompting the

cybercriminal(s) behind it to [3]**redirect all the campaign traffic to my Blogger profile?**

It appears that the cybercriminal/gang of cybercriminals behind these mass Web site compromise campaigns

is/are not just [4]**still in business**, but also – Long Tail of the malicious Web – [5]**managed to infect FireEye' (external network) Careers Web Site.**

Let's dissect the campaign, expose the malicious domains portfolio behind it, provide MD5s for a sample ex-

exploit, the dropped malware, and connect it to related malicious campaigns, all of which continue to share the same malicious infrastructure.

Sample redirection chain:

hxxp://vjs.zencdn.net/c/video.js

->

hxxp://cdn.adsbarscript.com/links/jump/

(198.7.59.235;

63.247.93.69;

69.39.238.28;

74.81.94.44)

(IE)

->

hxxp://cdn.adsbarscript.com/links/flash/?updnew

(CHROME)

->

*hxxp://209.239.127.185/591918d6c2e8ce3f53ed8b93fb0735
cd/face-book.php*

Detection rate for a sample malicious script found on the client-side exploits serving site:

[6]MD5: 809f70b26e3a50fb9146ddfa8cf500be - detected by 1 out of 49 antivirus scanners as Trojan.Script.Heuristic-

js.iacgm

Sample detection rate for the served client-side exploit:

[7]MD5: 71c92ebc2a889d3541ff6f20b4740868 - detected by 4 out of 49 antivirus scanners as HEUR:Exploit.Java.CVE-2012-1723.gen; HEUR_JAVA.EXEC

Detection rate for a sample dropped malware:

[8]MD5:

4bfb3379a2814f5eb67345d43bce3091 - detected by 15 out of 49 antivirus scanners as Trojan-

PSW.Win32.Fareit.acqv; PWS:Win32/Fareit.gen!C

The following malicious MD5s are known to have been downloaded from the same IPs (cdn.adsbarscript.com

(198.7.59.235; 63.247.93.69; 69.39.238.28; 74.81.94.44):

[9]MD5: 82e1013106736b74255586169a217d66

[10]MD5: 01771c3500a5b1543f4fb43945337c7d

[11]MD5: dbf6f5373f56f67e843af30fded5c7f2

701

Additionally, the campaign is also known to have dropped

[12]MD5: 01771c3500a5b1543f4fb43945337c7d

Once executed, the most recently dropped sample (MD5:

4bfb3379a2814f5eb67345d43bce3091) phones

back to the following C &C servers:

main-firewalls.com (67.228.177.174; 74.204.171.69; 85.195.104.90) - Email: alex1978a@bigmir.net

simple-cdn-node.com (109.120.143.109) - Email: alex1978a@bigmir.net

akamai.com/gate.php

Deja vu! We've already seen alex1978a@bigmir.net in [13]**Network Solution's (2010) mass Wordpress blogs**

compromise, a campaign which is also directly connected with [14]**the compromise of the Web site of the U.S**

Treasury.

The sample also attempts to download the following additional malware variants:

main-firewalls.com/6.exe

main-firewalls.com/1.exe

simple-cdn-node.com/1.exe - [15]**MD5: 05d003a374a29c9c2bbc250dd5c56d7c**

Responding to 67.228.177.174 are also the following malicious domains:

aodairangdong.com

bolsaminimall.com

catch-cdn.com

corp-firewall.com

himarkrealty.com

ngnetworld.com

ritz-entertainment.com

server.evietmusic.com

viettv24.com

vpoptv.com

plussolarsolutions.com

artistflower.com

autoairsystems.com

eighteas.com

greenpowersurvey.com

phattubi.com

ritz-entertainment.com

saigoncitymall.com

The following malicious MD5s are also known to have phoned back to the same IP (67.228.177.174) in the past:

MD5: 05636d38090e5726077cea54d2485806

MD5: 53b73675f1b08cf7ecfc3c80677c8d2e

MD5: 0f424ff9db97dafaba746f26d6d8d5c0

MD5: 633d6de861edc2ecf667f02d0997f10e

MD5: d13ead2b8a424b5e9c5977f8715514c4

MD5: bfc9803c94cc8ba76a916f8e915042e4

MD5: a04d33ced90f72c1a77f312708681c07

MD5: 7e6e15518cc48639612aa4ff00a2a454

MD5: 98d78ef8cc5aee193a7b7a3c3bb58c87

MD5: a030d6e35d736db9dd433a8d2ac8a915

702

MD5: 1f7a6ed70be6e13efb45e5ba80eed76e

MD5: cfc727a0ad51eb1f111305873d2ade04

MD5: 1b6de030ed3b42e939690630f63d6933

MD5: fa9e92d42580e1789ed04e551a379e4e

MD5: 2ed9d63e4d557667bad7806872cf4412

MD5: bef16d25b2cada2a388ea06c204b44f3

MD5: 77a93ba48d6532e069745bca117d26ed

MD5: 7c7e4cef8a7181f7982a841f7f752368

MD5: 57b5e6f38998e32fa93856970cc66c5e

MD5: 5d388b1f2bf2dc9493f5c4cfb9d53ca0

MD5: ec24a959e39c5d2eb7dc769f4b098efb

MD5: 6357085196499ef5301548ff17b62619

MD5: 3173d4be34f489a4630f2439f9653c2c

MD5: 3bd239ee46ab8ba02f57ed1762bd3ae6

MD5: dce3e33eb294f0a7688be5bea6b7e9d4

MD5: 1ed678e9d29c25043fdd1b4c44f5b2ea

MD5: eccce6f5f509f4ef986d426445a98f0d

MD5: 74e1e2f2d562ab6883124cfa43300cf2

MD5: 6922efa2e5aa16b78c982d633cbe44e9

Responding to 85.195.104.90 are also the following malicious domains:

catch-cdn.com

corp-firewall.com

kronoemail.com

main-firewalls.com

viacominfosys.com

emaildatastore.com

The following malicious MD5s are also known to have phoned back to the same IP (85.195.104.90) in the past:

MD5: 88110dbce9591b68b06b859e7965d509

MD5: 0e055888564fb59cb6d4e35a5c5fb33d

MD5: e9d8d2842b576fd4f6ef9dde1fea4b9f

MD5: e750031fc9b9264852133d8f7284ac7a

MD5: e0da2ca4e9a174cd3c6f8a348e4861ad

MD5: b23a579d7b8bf5a03c121d2f74234b2d

MD5: a1ee5246d984d900f27ce94fbfc37c2b

MD5: 2118a70a2ccf0a7772725e765ad64e08

MD5: f26848e64040b4b6614d95bd967045df

MD5: 9c5997b32bea6945f0cb9ff0c18cf040

MD5: 353305483087a5316fd75f63d641ec1f

MD5: 34e67771ca411b163866f1e795b2e72e

MD5: 571e04b5af915979efc5a7f77794facb

MD5: a21df3ee0c9dd87cf6ca66581aa7eb76

MD5: e2137edd5f550b1942c16e70095c436b

MD5: 97437f6d670db2596b6a6b53c887055c

Such type of factual attribution based on gathered historical OSINT, isn't surprising, thanks to the fact that de-

spite the increasing number of novice cybercriminals joining the ecosystem, the "usual suspects" continue operating for the sake of achieving their fraudulent and malicious objectives.

This post has been reproduced from [16]Dancho Danchev's blog . Follow him [17]on Twitter.

1. <http://ddanchev.blogspot.com/2010/04/dissecting-wordpress-blogs-compromise.html>
2. <http://ddanchev.blogspot.com/2010/05/us-treasury-site-compromise-linked-to.html>
3.
http://1.bp.blogspot.com/_wICHhTiQmrA/S-CnwKJy7II/AAAAAAAAAEsA/3esPISPhaKc/s1600/BureauOfEngravingAndPrinting_exploits_malware_1.png
4. <http://blog.videojs.com/post//unauthorized-modification-of-video-js-cdn-files>
5. <http://www.fireeye.com/blog/technical/cyber-exploits/2013/09/darkleech-says-hello.html>
6.
<https://www.virustotal.com/en/file/311c27de8d357d9cbe63cbf798abad294d2daa467d45b7fb4b9bef4f613d0f33/analysis/1379521024/>
7.
<https://www.virustotal.com/en/file/a87d2556c8270d35d0dc49a29376fb50d685d05782cd48f376479a6217474b51/analysis/1379521163/>

8.

<https://www.virustotal.com/en/file/370ecf6b98a13b5b379cf1deedb5926fdb23dd9bac036087ca1d8a11e2eda8f8/analysis/>

[is/](#)

9.

<https://www.virustotal.com/en/file/e40a7604c087a709ec9b9f8a78564d1542c4d221733eb4ebb512b3d5202a8e1d/analysis/>

[is/](#)

10.

<https://www.virustotal.com/en/file/ea3be0fb4367e038c602a3de5811821d2367f3326ab2a12f469db4cda06fafa7/analysis/>

[is/](#)

11.

<https://www.virustotal.com/en/file/59d5d28ac1b169bfc390501fc9d29b5511dec357345df5e38c5aa47675acd5df/analysis/>

[is/](#)

12.

<https://www.virustotal.com/en/file/ea3be0fb4367e038c602a3de5811821d2367f3326ab2a12f469db4cda06fafa7/analysis/>

[is/](#)

13. <http://ddanchev.blogspot.com/2010/04/dissecting-wordpress-blogs-compromise.html>

14. <http://ddanchev.blogspot.com/2010/05/us-treasury-site-compromise-linked-to.html>

15.

<https://www.virustotal.com/en/file/e28f368359094d42110fba>

e6bbef5cca649eac4ba540192827cac7b794bdaab7/analysis/

16. <http://ddanchev.blogspot.com/>

17. <http://twitter.com/danchodanchev>

704

```

121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400 401 402 403 404 405 406 407 408 409 410 411 412 413 414 415 416 417 418 419 420 421 422 423 424 425 426 427 428 429 430 431 432 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448 449 450 451 452 453 454 455 456 457 458 459 460 461 462 463 464 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 480 481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496 497 498 499 500 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544 545 546 547 548 549 550 551 552 553 554 555 556 557 558 559 560 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576 577 578 579 580 581 582 583 584 585 586 587 588 589 590 591 592 593 594 595 596 597 598 599 600 601 602 603 604 605 606 607 608 609 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624 625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 640 641 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688 689 690 691 692 693 694 695 696 697 698 699 700 701 702 703 704 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 720 721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736 737 738 739 740 741 742 743 744 745 746 747 748 749 750 751 752 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768 769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 790 791 792 793 794 795 796 797 798 799 800 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816 817 818 819 820 821 822 823 824 825 826 827 828 829 830 831 832 833 834 835 836 837 838 839 840 841 842 843 844 845 846 847 848 849 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864 865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 880 881 882 883 884 885 886 887 888 889 890 891 892 893 894 895 896 897 898 899 900 901 902 903 904 905 906 907 908 909 910 911 912 913 914 915 916 917 918 919 920 921 922 923 924 925 926 927 928 929 930 931 932 933 934 935 936 937 938 939 940 941 942 943 944 945 946 947 948 949 950 951 952 953 954 955 956 957 958 959 960 961 962 963 964 965 966 967 968 969 970 971 972 973 974 975 976 977 978 979 980 981 982 983 984 985 986 987 988 989 990 991 992 993 994 995 996 997 998 999 1000

```

Dissecting FireEye's Career Web Site Compromise (2013-09-18 19:41)

Remember when back in 2010, I established a direct connection between several [1]**mass Wordpress blogs com-**

promise campaigns, with the campaign behind the [2]**compromised Web site of the U.S. Treasury**, prompting the

cybercriminal(s) behind it to [3]**redirect all the campaign traffic to my Blogger profile?**

It appears that the cybercriminal/gang of cybercriminals behind these mass Web site compromise campaigns

is/are not just [4]**still in business**, but also – Long Tail of the malicious Web – [5]**managed to infect FireEye'**

(external network) Careers Web Site.

Let's dissect the campaign, expose the malicious domains portfolio behind it, provide MD5s for a sample ex-

ploit, the dropped malware, and connect it to related malicious campaigns, all of which continue to share the same malicious infrastructure.

Sample redirection chain:

hxxp://vjs.zencdn.net/c/video.js

->

hxxp://cdn.adsbarscript.com/links/jump/

(198.7.59.235;

63.247.93.69;

69.39.238.28;

74.81.94.44)

(IE)

->

hxxp://cdn.adsbarscript.com/links/flash/?updnew

(CHROME)

->

*hxxp://209.239.127.185/591918d6c2e8ce3f53ed8b93fb0735
cd/face-book.php*

Detection rate for a sample malicious script found on the client-side exploits serving site:

[6]MD5: 809f70b26e3a50fb9146ddfa8cf500be - detected by 1 out of 49 antivirus scanners as Trojan.Script.Heuristic-js.iacgm

Sample detection rate for the served client-side exploit:

[7]MD5: 71c92ebc2a889d3541ff6f20b4740868 - detected by 4 out of 49 antivirus scanners as HEUR:Exploit.Java.CVE-2012-1723.gen; HEUR_JAVA.EXEC

Detection rate for a sample dropped malware:

[8]MD5: 4bfb3379a2814f5eb67345d43bce3091 - detected by 15 out of 49 antivirus scanners as Trojan-PSW.Win32.Fareit.acqv; PWS:Win32/Fareit.gen!C

The following malicious MD5s are known to have been downloaded from the same IPs (cdn.adsbarscript.com)

(198.7.59.235; 63.247.93.69; 69.39.238.28; 74.81.94.44):

[9]MD5: 82e1013106736b74255586169a217d66

[10]MD5: 01771c3500a5b1543f4fb43945337c7d

[11]MD5: dbf6f5373f56f67e843af30fded5c7f2

705

Additionally, the campaign is also known to have dropped
[12]**MD5: 01771c3500a5b1543f4fb43945337c7d**

**Once executed, the most recently dropped sample
(MD5:**

4bfb3379a2814f5eb67345d43bce3091) phones

back to the following C &C servers:

main-firewalls.com (67.228.177.174; 74.204.171.69;
85.195.104.90) - Email: alex1978a@bigmir.net

simple-cdn-node.com (109.120.143.109) - Email:
alex1978a@bigmir.net

akamai.com/gate.php

Deja vu! We've already seen alex1978a@bigmir.net in
[13]**Network Solution's (2010) mass Wordpress blogs**

compromise, a campaign which is also directly connected
with [14]**the compromise of the Web site of the U.S**

Treasury.

**The sample also attempts to download the following
additional malware variants:**

main-firewalls.com/6.exe

main-firewalls.com/1.exe

simple-cdn-node.com/1.exe - [15]**MD5:
05d003a374a29c9c2bbc250dd5c56d7c**

Responding to 67.228.177.174 are also the following malicious domains:

aodairangdong.com

bolsaminimall.com

catch-cdn.com

corp-firewall.com

himarkrealty.com

ngnetworld.com

ritz-entertainment.com

server.evietmusic.com

viettv24.com

vpoptv.com

plussolarsolutions.com

artistflower.com

autoairsystems.com

eighteas.com

greenpowersurvey.com

phattubi.com

ritz-entertainment.com

saigoncitymall.com

The following malicious MD5s are also known to have phoned back to the same IP (67.228.177.174) in the past:

MD5: 05636d38090e5726077cea54d2485806

MD5: 53b73675f1b08cf7ecfc3c80677c8d2e

MD5: 0f424ff9db97dafaba746f26d6d8d5c0

MD5: 633d6de861edc2ecf667f02d0997f10e

MD5: d13ead2b8a424b5e9c5977f8715514c4

MD5: bfc9803c94cc8ba76a916f8e915042e4

MD5: a04d33ced90f72c1a77f312708681c07

MD5: 7e6e15518cc48639612aa4ff00a2a454

MD5: 98d78ef8cc5aee193a7b7a3c3bb58c87

MD5: a030d6e35d736db9dd433a8d2ac8a915

706

MD5: 1f7a6ed70be6e13efb45e5ba80eed76e

MD5: cfc727a0ad51eb1f111305873d2ade04

MD5: 1b6de030ed3b42e939690630f63d6933

MD5: fa9e92d42580e1789ed04e551a379e4e

MD5: 2ed9d63e4d557667bad7806872cf4412

MD5: bef16d25b2cada2a388ea06c204b44f3

MD5: 77a93ba48d6532e069745bca117d26ed

MD5: 7c7e4cef8a7181f7982a841f7f752368

MD5: 57b5e6f38998e32fa93856970cc66c5e

MD5: 5d388b1f2bf2dc9493f5c4cfb9d53ca0

MD5: ec24a959e39c5d2eb7dc769f4b098efb

MD5: 6357085196499ef5301548ff17b62619

MD5: 3173d4be34f489a4630f2439f9653c2c

MD5: 3bd239ee46ab8ba02f57ed1762bd3ae6

MD5: dce3e33eb294f0a7688be5bea6b7e9d4

MD5: 1ed678e9d29c25043fdd1b4c44f5b2ea

MD5: eccce6f5f509f4ef986d426445a98f0d

MD5: 74e1e2f2d562ab6883124cfa43300cf2

MD5: 6922efa2e5aa16b78c982d633cbe44e9

Responding to 85.195.104.90 are also the following malicious domains:

catch-cdn.com

corp-firewall.com

kronoemail.com

main-firewalls.com

viacominfosys.com

emaildatastore.com

The following malicious MD5s are also known to have phoned back to the same IP (85.195.104.90) in the past:

MD5: 88110dbce9591b68b06b859e7965d509

MD5: 0e055888564fb59cb6d4e35a5c5fb33d

MD5: e9d8d2842b576fd4f6ef9dde1fea4b9f

MD5: e750031fc9b9264852133d8f7284ac7a

MD5: e0da2ca4e9a174cd3c6f8a348e4861ad

MD5: b23a579d7b8bf5a03c121d2f74234b2d

MD5: a1ee5246d984d900f27ce94fbfc37c2b

MD5: 2118a70a2ccf0a7772725e765ad64e08

MD5: f26848e64040b4b6614d95bd967045df

MD5: 9c5997b32bea6945f0cb9ff0c18cf040

MD5: 353305483087a5316fd75f63d641ec1f

MD5: 34e67771ca411b163866f1e795b2e72e

MD5: 571e04b5af915979efc5a7f77794facb

MD5: a21df3ee0c9dd87cf6ca66581aa7eb76

MD5: e2137edd5f550b1942c16e70095c436b

MD5: 97437f6d670db2596b6a6b53c887055c

Such type of factual attribution based on gathered historical OSINT, isn't surprising, thanks to the fact that de-

spite the increasing number of novice cybercriminals joining the ecosystem, the "usual suspects" continue operating for the sake of achieving their fraudulent and malicious objectives.

707

Updates will be posted as soon as new developments take place.

1. <http://ddanchev.blogspot.com/2010/04/dissecting-wordpress-blogs-compromise.html>

2. <http://ddanchev.blogspot.com/2010/05/us-treasury-site-compromise-linked-to.html>

3.

[http://1.bp.blogspot.com/_wIcHhTiQmrA/S-CnwKJy7II/AAAAAAAAAEsA/3esPISPhaKc/s1600/BureauOfEngravingAndPrint](http://1.bp.blogspot.com/_wIcHhTiQmrA/S-CnwKJy7II/AAAAAAAAAEsA/3esPISPhaKc/s1600/BureauOfEngravingAndPrinting_exploits_malware_1.png)

[ing_exploits_malware_1.png](#)

4. <http://blog.videojs.com/post//unauthorized-modification-of-video-js-cdn-files>

5. <http://www.fireeye.com/blog/technical/cyber-exploits/2013/09/darkleech-says-hello.html>

6.

<https://www.virustotal.com/en/file/311c27de8d357d9cbe63cbf798abad294d2daa467d45b7fb4b9bef4f613d0f33/analysis/1379521024/>

7.

<https://www.virustotal.com/en/file/a87d2556c8270d35d0dc49a29376fb50d685d05782cd48f376479a6217474b51/analysis/1379521163/>

8.

<https://www.virustotal.com/en/file/370ecf6b98a13b5b379cf1deedb5926fdb23dd9bac036087ca1d8a11e2eda8f8/analysis/>

9.

<https://www.virustotal.com/en/file/e40a7604c087a709ec9b9f8a78564d1542c4d221733eb4ebb512b3d5202a8e1d/analysis/>

10.

<https://www.virustotal.com/en/file/ea3be0fb4367e038c602a3de5811821d2367f3326ab2a12f469db4cda06fafa7/analysis/>

11.

<https://www.virustotal.com/en/file/59d5d28ac1b169bfc390501fc9d29b5511dec357345df5e38c5aa47675acd5df/analysis/>

12.

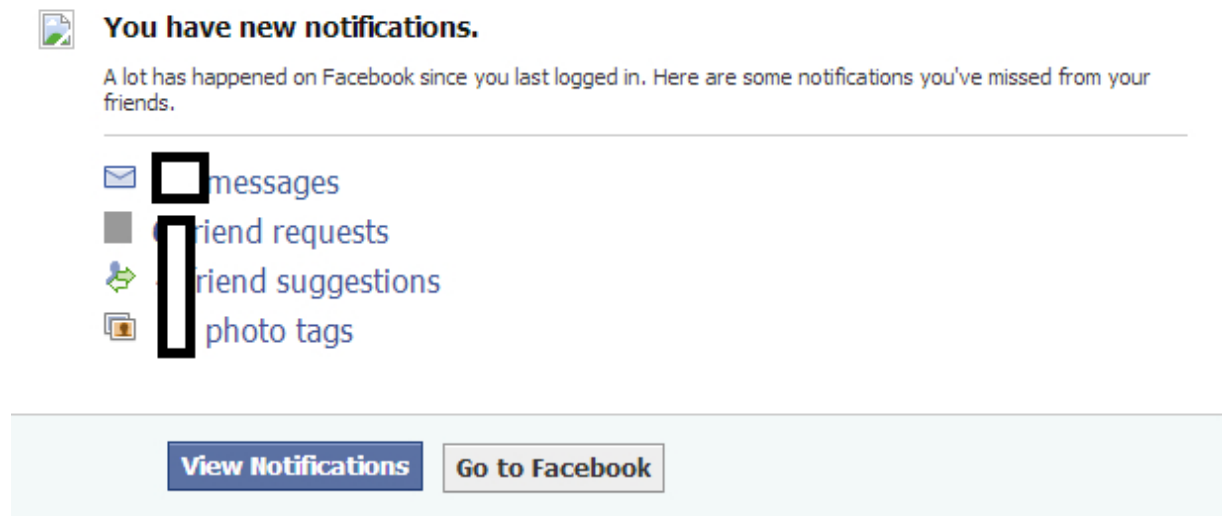
<https://www.virustotal.com/en/file/ea3be0fb4367e038c602a3de5811821d2367f3326ab2a12f469db4cda06fafa7/analysis/>

13. <http://ddanchev.blogspot.com/2010/04/dissecting-wordpress-blogs-compromise.html>

14. <http://ddanchev.blogspot.com/2010/05/us-treasury-site-compromise-linked-to.html>

15. <https://www.virustotal.com/en/file/e28f368359094d42110fbae6bbef5cca649eac4ba540192827cac7b794bdaab7/analysis/>

708



This message was sent to [REDACTED] If you don't want to receive these emails from Facebook in the future, please [unsubscribe](#).
Facebook, Inc., Attention: Department 415, PO Box 10005, Palo Alto, CA 94303

Spamvertised Facebook 'You have friend suggestions, friend requests and photo tags' Themed Emails

Lead to Client-side Exploits and Malware (2013-09-28 13:53)

A currently circulating malicious 'Facebook notifications' themed spam campaign, attempts to trick Facebook's users

into thinking that they've received a notifications digest for the activity that (presumably) took place while they were

logged out of Facebook. In reality though, once users click on any of the links found in the malicious email, they're

automatically exposed to client-side exploits ultimately dropping malware on their hosts.

Let's dissect the campaign, provide actionable intelligence on the campaign's structure, the involved portfolio

of malicious domains, actual/related MD5s, and as always, connect the currently ongoing campaign with two other

previously profiled malicious campaigns.

Spamvertised URL:

`hxxp://user4634.vs.easily.co.uk/darkened/PSEUDO_RANDOM_CHARACTERS`

Attempts to load the following malicious scripts:

`hxxp://3dbrandscapes.com/starker/manipulator.js`

`hxxp://distrigold.eu/compounding/melisa.js`

`hxxp://ly-ra.com/shallot/mandalay.js`

Client-side exploits serving URL:

`hxxp://directgrid.org/topic/lairtg-nilles-slliks.php`

Malicious domain name reconnaissance:

directgrid.org - 50.116.10.71 - Email:
ringfields@islandresearch.net

Responding to the following IP (50.116.10.71) are also the following malicious domains participating in the

campaign:

directgrid.biz

709

directgrid.com

directgrid.info

directgrid.net

directgrid.org

directgrid.us

gilkjones.com

integra-inspection.ca

integra-inspection.co

integra-inspection.info

taxipunjab.com

taxisamritsar.com

watttrack.com

The following malicious MD5s are known to have been downloaded - related campaigns - from the same

IP (50.116.10.71):

MD5: 7eb6740ed6935da49614d95a43146dea

MD5: 7768f7039988236165cdd5879934cc5d

**The following malicious MD5s are known to have
'phoned back' to the same IP (50.116.10.71) over the
past**

24 hours:

MD5: a0065f7649db9a885acd34301ae863b0

MD5: 5503573f4fe15b211956f67c66e18d02

MD5: 01d757b672673df8032abbaa8acf3e22

MD5: 7ad68895e5ec9d4f53fc9958c70df01a

MD5: fd99250ecb845a455499db8df1780807

MD5: fd99250ecb845a455499db8df1780807

MD5: 3983170d46a130f23471340a47888c93

MD5: c86c79d9fee925a690a4b0307d7f2329

MD5: 25f498f7823f12294c685e9bc79376d2

MD5: 470f4aa3f76ea3b465741a73ce6c22fe

MD5: 43b78852a7363d8a4cf7538d4e68c887

MD5: e3aae430ed4036b19f26fa2ed9bbe2bf

MD5: e782619301a0a0a843cedc5d02c563b5

MD5: fc16335d0e1827b271b031309634dc0f

MD5: a55e21b0231d0508cb638892b6ee8ec5

MD5: 053c84c12900b81506eb884ec9f930c9

MD5: e03d0dd786b038c570dc53690db0673b

MD5: 086b16af34857cb5dfb0163cc1c92569

MD5: e066b50bae491587574603bdfd60826e

MD5: eb22137880f8c5a03c73135f288afb8a

MD5: b88392fb63747668c982b6321e5ce712

MD5: 6254d901b1566bef94e673f833adff8c

MD5: 258d640b802a0bbe08471f4f064cb94a

MD5: c1cefb742107516c3a73489eae176745

MD5: a19f1d5c98c2d7f036f2693ad6c14626

MD5: 3f02f35bc73ad9ef14ab4f960926fd45

**Sample detection rate for the client-side exploits
serving malicious script:**

[1]MD5: 00f5d150ff1b50c0bbc1d038eb676c29 -
detected by 2 out of 48 antivirus scanners as
Script.Exploit.Kit.C;

Troj/ObfJS-EO



Sample detection rate for the served exploit:

[2]MD5:

d49275523cae83a5e7639bb22604dd86 - detected by 5 out of 48 antivirus scanners as

HEUR:Exploit.Java.Generic; HEUR _JAVA.EXEC; TROJ _GEN.F47V0927

Upon successful client-side exploitation the campaign drops the following malicious sample on the affected

hosts:

[3]MD5: 6ef9476e6227ef631b231b66d7a2a08b - detected by 7 out of 48 antivirus scanners as Win32/Spy.Zbot.AAU;

Trojan-Spy.Win32.Zbot.qckm; TROJ _GEN.F47V0927

Once executed, the sample starts listening on ports 3185 and 7101.

It also creates the following Mutexes on the system:

Local\ {B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A }

Local\ {B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A }

Local\ {D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A }

Local\ {D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A }

Local\ {0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A }

Local\ {911F9FCD-AFAC-6AF2-DBC9-BE58FA349D4A }

Global\ {2E06BA86-8AE7-D5EB-DBC9-BE58FA349D4A }

Global\ {B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A }

Global\ {B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A }

Global\ {D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A }

Global\ {D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A }

Global\ {0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A }

Global\ {BB67AFC4-9FA5-408A-DBC9-BE58FA349D4A }

Global\ {3DC7903B-A05A-C62A-11EB-B06D3016937F }

Global\ {3DC7903B-A05A-C62A-75EA-B06D5417937F }

Global\ {3DC7903B-A05A-C62A-4DE9-B06D6C14937F }

711

Global\ {3DC7903B-A05A-C62A-65E9-B06D4414937F }

Global\ {3DC7903B-A05A-C62A-89E9-B06DA814937F }

Global\ {3DC7903B-A05A-C62A-BDE9-B06D9C14937F }

Global\ {3DC7903B-A05A-C62A-51E8-B06D7015937F }

Global\ {3DC7903B-A05A-C62A-81E8-B06DA015937F }

Global\ {3DC7903B-A05A-C62A-FDE8-B06DDC15937F }

Global\ {3DC7903B-A05A-C62A-0DEF-B06D2C12937F }

Global\ {3DC7903B-A05A-C62A-5DEF-B06D7C12937F }

Global\ {3DC7903B-A05A-C62A-95EE-B06DB413937F }

Global\ {3DC7903B-A05A-C62A-F1EE-B06DD013937F }

Global\ {3DC7903B-A05A-C62A-89EB-B06DA816937F }

Global\ {3DC7903B-A05A-C62A-F9EF-B06DD812937F }

Global\ {3DC7903B-A05A-C62A-E5EF-B06DC412937F }

Global\ {3DC7903B-A05A-C62A-0DEE-B06D2C13937F }

Global\ {3DC7903B-A05A-C62A-09ED-B06D2810937F }

Global\ {3DC7903B-A05A-C62A-51EF-B06D7012937F }

Global\ {3DC7903B-A05A-C62A-35EC-B06D1411937F }

Global\ {3DC7903B-A05A-C62A-55EF-B06D7412937F }

Global\ {DDB39BDC-ABBD-265E-DBC9-BE58FA349D4A }

Global\ {2E1C200D-106C-D5F1-DBC9-BE58FA349D4A }

MPSWabDataAccessMutex

MPSWABOIkStoreNotifyMutex

The following Registry Keys:

HKEY_CURRENT_USER\Software\Microsoft\Waosumag

And changes the following Registry Values:

[HKEY_CURRENT_USER\Identities] -> Identity Login = 0x00098053

*[HKEY_CURRENT_USER\Software\Microsoft\Windows
textbackslashCurrentVersion\Run] -> Keby = "" %AppData
%\Ortuet\keby.exe""*

*[HKEY_CURRENT_USER\Software\Microsoft\Waosumag] ->
2df3e6ig = 23 CD 87 C3 1E D1 FA C6 28 2E DF 4D 12 21;*

*2icbbj3a = 0xC3E6CD13; 185cafc2 = CB D5 E6 C3 F6 D8 CD
C6 05 2E EF 4D*

It then phones back to the following C &C (command and control) servers:

99.157.164.179

174.76.94.24

99.60.68.114

217.35.75.232

184.145.205.63

99.60.111.51

207.47.212.146

108.240.232.212

107.193.222.108

173.202.183.58

201.170.83.92

81.136.188.57

71.186.174.184

We've already seen the same IPs (217.35.75.232; 108.240.232.212) in the following previously profiled mali-

cious campaign - [4]**Spamvertised "FDIC: Your business account" themed emails serve client-side exploits and**

712

malware.

We've also seen (107.193.222.108) in the following malicious campaign - [5]**Spamvertised 'Export License/Invoice**

Copy' themed emails lead to malware, indicating that all of these campaigns are controlled using the same malicious botnet infrastructure.

The following malicious MD5s are also known to have phoned back to the same C &C servers used in this

campaign, over the past 24 hours:

MD5: 9f550edbb505e22b0203e766bd1b9982

MD5: 46cdaead83d9e3de803125e45ca88894

MD5: ffe07e0997d8ec82feb81bac53838d6d

MD5: 28c0bc772aec891a08b06a4029230626

MD5: c8055c6668d1c4c9cb9d68c2c09c14d4

MD5: 0bbabb722e1327cbe903ab477716ae2e

MD5: c4c5db70e7c971e3e556eb9d65f87c84

MD5: 0ff4d450ce9b1eaaef5ed9a5a1fa392d

MD5: e01f435a8c5ed93f6800971505a2cdd2

MD5: 042508083351b79f01a4d7b7e8e35826

MD5: 1f5f75ae82d6aa7099315bf19d0ae4e0

MD5: 35c4d4c2031157645bb3a1e4e709edeb

MD5: a0065f7649db9a885acd34301ae863b0

MD5: 5503573f4fe15b211956f67c66e18d02

MD5: 01d757b672673df8032abbaa8acf3e22

MD5: fd99250ecb845a455499db8df1780807

MD5: 1fab971283479b017dfb79857ecd343b

MD5: a130cddd61dad9188b9b89451a58af28

MD5: 2af94e79f9b9ee26032ca863a86843be

MD5: 8b03a5cf4f149ac7696d108bff586cc5

MD5: 802a522405076d7f8b944b781e4fe133

MD5: b9c7d2466a689365ebb8f6f607cd3368

MD5: 43b78852a7363d8a4cf7538d4e68c887

MD5: c62b6206e9eefe75ba1804788dc552f7

MD5: 385b5358f6a1f15706b536a9dc5b1590

MD5: e3aae430ed4036b19f26fa2ed9bbe2bf

MD5: e782619301a0a0a843cedc5d02c563b5

MD5: fc16335d0e1827b271b031309634dc0f

MD5: 4850969b7febc82c8b82296fa129e818

MD5: 203e0acced8a76560312b452d70ff1e7

MD5: a55e21b0231d0508cb638892b6ee8ec5

MD5: edb1a26ebb8ab5df780b643ad1f0d50f

MD5: 053c84c12900b81506eb884ec9f930c9

MD5: e03d0dd786b038c570dc53690db0673b

MD5: 47d4804fda31b6f88b0d33b86fc681ae

MD5: 086b16af34857cb5dfb0163cc1c92569

This post has been reproduced from [6]Dancho Danchev's blog . Follow him [7]on Twitter.

1.

<https://www.virustotal.com/en/file/95d3cfd6c1f094871f311593c73726700a1fcc7a1f5cf13ced1317c040545873/analysis/1380362621/>

2.

<https://www.virustotal.com/en/file/bd7c0f52fd7d7e9b20ab9e>

[8f13ac114243a4f09433f484f8fbc3b51c7c44650d/analys](#)

[713](#)

[is/](#)

3.

[https://www.virustotal.com/en/file/8b0e0b269a2e332bae756304c07f392789f1c0215c2b23d52cc13fb1ae49f076/analys](#)

[is/1380320726/](#)

4. [http://www.webroot.com/blog/2013/09/23/spamvertised-fdic-business-account-themed-emails-server-client-sid](#)

[e-exploits-malware/](#)

5. [http://www.webroot.com/blog/2013/07/09/spamvertised-export-licenseinvoice-copy-themed-emails-lead-to-malw](#)

[are/](#)

6. [http://ddanchev.blogspot.com/](#)

7. [http://twitter.com/danchodanchev](#)

714



You have new notifications.

A lot has happened on Facebook since you last logged in. Here are some notifications you've missed from your friends.



messages



friend requests



friend suggestions



photo tags

[View Notifications](#)

[Go to Facebook](#)

This message was sent to [REDACTED] If you don't want to receive these emails from Facebook in the future, please [unsubscribe](#).

Facebook, Inc., Attention: Department 415, PO Box 10005, Palo Alto, CA 94303

Spamvertised Facebook 'You have friend suggestions, friend requests and photo tags' Themed Emails

Lead to Client-side Exploits and Malware (2013-09-28 13:53)

A currently circulating malicious 'Facebook notifications' themed spam campaign, attempts to trick Facebook's users

into thinking that they've received a notifications digest for the activity that (presumably) took place while they were

logged out of Facebook. In reality though, once users click on any of the links found in the malicious email, they're

automatically exposed to client-side exploits ultimately dropping malware on their hosts.

Let's dissect the campaign, provide actionable intelligence on the campaign's structure, the involved portfolio

of malicious domains, actual/related MD5s, and as always, connect the currently ongoing campaign with two other previously profiled malicious campaigns.

Spamvertised URL:

hxxp://user4634.vs.easily.co.uk/darkened/PSEUDO_RANDOM_CHARACTERS

Attempts to load the following malicious scripts:

hxxp://3dbrandscapes.com/starker/manipulator.js

hxxp://distrigold.eu/compounding/melisa.js

hxxp://ly-ra.com/shallot/mandalay.js

Client-side exploits serving URL:

hxxp://directgrid.org/topic/lairtg-nilles-slliks.php

Malicious domain name reconnaissance:

directgrid.org - 50.116.10.71 - Email:
ringfields@islandresearch.net

Responding to the following IP (50.116.10.71) are also the following malicious domains participating in the

campaign:

directgrid.biz

715

directgrid.com

directgrid.info

directgrid.net

directgrid.org

directgrid.us

gilkjones.com

integra-inspection.ca

integra-inspection.co

integra-inspection.info

taxipunjab.com

taxisamritsar.com

watttrack.com

The following malicious MD5s are known to have been downloaded - related campaigns - from the same

IP (50.116.10.71):

MD5: 7eb6740ed6935da49614d95a43146dea

MD5: 7768f7039988236165cdd5879934cc5d

The following malicious MD5s are known to have 'phoned back' to the same IP (50.116.10.71) over the past

24 hours:

MD5: a0065f7649db9a885acd34301ae863b0

MD5: 5503573f4fe15b211956f67c66e18d02

MD5: 01d757b672673df8032abbaa8acf3e22

MD5: 7ad68895e5ec9d4f53fc9958c70df01a

MD5: fd99250ecb845a455499db8df1780807

MD5: fd99250ecb845a455499db8df1780807

MD5: 3983170d46a130f23471340a47888c93

MD5: c86c79d9fee925a690a4b0307d7f2329

MD5: 25f498f7823f12294c685e9bc79376d2

MD5: 470f4aa3f76ea3b465741a73ce6c22fe

MD5: 43b78852a7363d8a4cf7538d4e68c887

MD5: e3aae430ed4036b19f26fa2ed9bbe2bf

MD5: e782619301a0a0a843cedc5d02c563b5

MD5: fc16335d0e1827b271b031309634dc0f

MD5: a55e21b0231d0508cb638892b6ee8ec5

MD5: 053c84c12900b81506eb884ec9f930c9

MD5: e03d0dd786b038c570dc53690db0673b

MD5: 086b16af34857cb5dfb0163cc1c92569

MD5: e066b50bae491587574603bdfd60826e

MD5: eb22137880f8c5a03c73135f288afb8a

MD5: b88392fb63747668c982b6321e5ce712

MD5: 6254d901b1566bef94e673f833adff8c

MD5: 258d640b802a0bbe08471f4f064cb94a

MD5: c1cefb742107516c3a73489eae176745

MD5: a19f1d5c98c2d7f036f2693ad6c14626

MD5: 3f02f35bc73ad9ef14ab4f960926fd45

Sample detection rate for the client-side exploits serving malicious script:

[1]**MD5: 00f5d150ff1b50c0bbc1d038eb676c29** -
detected by 2 out of 48 antivirus scanners as
Script.Exploit.Kit.C;

Troj/ObfJS-EO

716



Sample detection rate for the served exploit:

[2]MD5:

d49275523cae83a5e7639bb22604dd86 - detected by 5 out of 48 antivirus scanners as

HEUR:Exploit.Java.Generic; HEUR _JAVA.EXEC; TROJ _GEN.F47V0927

Upon successful client-side exploitation the campaign drops the following malicious sample on the affected

hosts:

[3]MD5: 6ef9476e6227ef631b231b66d7a2a08b - detected by 7 out of 48 antivirus scanners as Win32/Spy.Zbot.AAU;

Trojan-Spy.Win32.Zbot.qckm; TROJ _GEN.F47V0927

Once executed, the sample starts listening on ports 3185 and 7101.

It also creates the following Mutexes on the system:

Local\ {B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A }

Local\ {B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A }

Local\ {D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A }

Local\ {D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A }

Local\ {0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A }

Local\ {911F9FCD-AFAC-6AF2-DBC9-BE58FA349D4A }

Global\ {2E06BA86-8AE7-D5EB-DBC9-BE58FA349D4A }

Global\ {B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A }

Global\ {B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A }

Global\ {D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A }

Global\ {D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A }

Global\ {0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A }

Global\ {BB67AFC4-9FA5-408A-DBC9-BE58FA349D4A }

Global\ {3DC7903B-A05A-C62A-11EB-B06D3016937F }

Global\ {3DC7903B-A05A-C62A-75EA-B06D5417937F }

Global\ {3DC7903B-A05A-C62A-4DE9-B06D6C14937F }

717

Global\ {3DC7903B-A05A-C62A-65E9-B06D4414937F }

Global\ {3DC7903B-A05A-C62A-89E9-B06DA814937F }

Global\ {3DC7903B-A05A-C62A-BDE9-B06D9C14937F }

Global\ {3DC7903B-A05A-C62A-51E8-B06D7015937F }

Global\ {3DC7903B-A05A-C62A-81E8-B06DA015937F }

Global\ {3DC7903B-A05A-C62A-FDE8-B06DDC15937F }

Global\ {3DC7903B-A05A-C62A-0DEF-B06D2C12937F }

Global\ {3DC7903B-A05A-C62A-5DEF-B06D7C12937F }

Global\ {3DC7903B-A05A-C62A-95EE-B06DB413937F }

Global\ {3DC7903B-A05A-C62A-F1EE-B06DD013937F }

Global\ {3DC7903B-A05A-C62A-89EB-B06DA816937F }

Global\ {3DC7903B-A05A-C62A-F9EF-B06DD812937F }
Global\ {3DC7903B-A05A-C62A-E5EF-B06DC412937F }
Global\ {3DC7903B-A05A-C62A-0DEE-B06D2C13937F }
Global\ {3DC7903B-A05A-C62A-09ED-B06D2810937F }
Global\ {3DC7903B-A05A-C62A-51EF-B06D7012937F }
Global\ {3DC7903B-A05A-C62A-35EC-B06D1411937F }
Global\ {3DC7903B-A05A-C62A-55EF-B06D7412937F }
Global\ {DDB39BDC-ABBD-265E-DBC9-BE58FA349D4A }
Global\ {2E1C200D-106C-D5F1-DBC9-BE58FA349D4A }
MPSWabDataAccessMutex
MPSWABOlKStoreNotifyMutex

The following Registry Keys:

HKEY_CURRENT_USER\Software\Microsoft\Waosumag

And changes the following Registry Values:

[HKEY_CURRENT_USER\Identities] -> Identity Login = 0x00098053

*[HKEY_CURRENT_USER\Software\Microsoft\Windows
textbackslashCurrentVersion\Run] -> Keby = "" %AppData
%\Ortuet\keby.exe""*

[HKEY_CURRENT_USER\Software\Microsoft\Waosumag] -> 2df3e6ig = 23 CD 87 C3 1E D1 FA C6 28 2E DF 4D 12 21;

*2icbbj3a = 0xC3E6CD13; 185cafc2 = CB D5 E6 C3 F6 D8 CD
C6 05 2E EF 4D*

It then phones back to the following C &C (command and control) servers:

99.157.164.179

174.76.94.24

99.60.68.114

217.35.75.232

184.145.205.63

99.60.111.51

207.47.212.146

108.240.232.212

107.193.222.108

173.202.183.58

201.170.83.92

81.136.188.57

71.186.174.184

We've already seen the same IPs (217.35.75.232; 108.240.232.212) in the following previously profiled mali-

cious campaign - [4]**Spamvertised "FDIC: Your business account" themed emails serve client-side exploits and**

718

malware.

We've also seen (107.193.222.108) in the following malicious campaign - [5]**Spamvertised 'Export License/Invoice**

Copy' themed emails lead to malware, indicating that all of these campaigns are controlled using the same malicious botnet infrastructure.

The following malicious MD5s are also known to have phoned back to the same C &C servers used in this campaign, over the past 24 hours:

MD5: 9f550edbb505e22b0203e766bd1b9982

MD5: 46cdaeadd83d9e3de803125e45ca88894

MD5: ffe07e0997d8ec82feb81bac53838d6d

MD5: 28c0bc772aec891a08b06a4029230626

MD5: c8055c6668d1c4c9cb9d68c2c09c14d4

MD5: 0bbabb722e1327cbe903ab477716ae2e

MD5: c4c5db70e7c971e3e556eb9d65f87c84

MD5: 0ff4d450ce9b1eaaef5ed9a5a1fa392d

MD5: e01f435a8c5ed93f6800971505a2cdd2

MD5: 042508083351b79f01a4d7b7e8e35826

MD5: 1f5f75ae82d6aa7099315bf19d0ae4e0

MD5: 35c4d4c2031157645bb3a1e4e709edeb

MD5: a0065f7649db9a885acd34301ae863b0

MD5: 5503573f4fe15b211956f67c66e18d02

MD5: 01d757b672673df8032abbaa8acf3e22

MD5: fd99250ecb845a455499db8df1780807

MD5: 1fab971283479b017dfb79857ecd343b

MD5: a130cddd61dad9188b9b89451a58af28

MD5: 2af94e79f9b9ee26032ca863a86843be

MD5: 8b03a5cf4f149ac7696d108bff586cc5

MD5: 802a522405076d7f8b944b781e4fe133

MD5: b9c7d2466a689365ebb8f6f607cd3368

MD5: 43b78852a7363d8a4cf7538d4e68c887

MD5: c62b6206e9eefe75ba1804788dc552f7

MD5: 385b5358f6a1f15706b536a9dc5b1590

MD5: e3aae430ed4036b19f26fa2ed9bbe2bf

MD5: e782619301a0a0a843cedc5d02c563b5

MD5: fc16335d0e1827b271b031309634dc0f

MD5: 4850969b7febc82c8b82296fa129e818

MD5: 203e0acced8a76560312b452d70ff1e7

MD5: a55e21b0231d0508cb638892b6ee8ec5

MD5: edb1a26ebb8ab5df780b643ad1f0d50f

MD5: 053c84c12900b81506eb884ec9f930c9

MD5: e03d0dd786b038c570dc53690db0673b

MD5: 47d4804fda31b6f88b0d33b86fc681ae

MD5: 086b16af34857cb5dfb0163cc1c92569

Updates will be posted as soon as new developments take place.

1.

<https://www.virustotal.com/en/file/95d3cfd6c1f094871f311593c73726700a1fcc7a1f5cf13ced1317c040545873/analysis/1380362621/>

719

2.

<https://www.virustotal.com/en/file/bd7c0f52fd7d7e9b20ab9e8f13ac114243a4f09433f484f8fbc3b51c7c44650d/analysis/>

3.

<https://www.virustotal.com/en/file/8b0e0b269a2e332bae756304c07f392789f1c0215c2b23d52cc13fb1ae49f076/analysis/1380320726/>

4. <http://www.webroot.com/blog/2013/09/23/spamvertised-fdic-business-account-themed-emails-server-client-sid-e-exploits-malware/>

5. <http://www.webroot.com/blog/2013/07/09/spamvertised-export-licenseinvoice-copy-themed-emails-lead-to-malware/>

720

1.10 October

721



Fake Pinterest 'Don't forget to confirm your email!' Themed Emails Serve Client-side Exploits and Malware (2013-10-01 21:12)

Cybercriminals have just launched yet another massive spam campaign, this time attempting to trick Pinterest users

into thinking that they've received an email confirmation request. In reality though, once users click on the links

found in the malicious emails, they're automatically exposed to client-side exploits, with the campaign dropping two

malware samples on the affected hosts once a successful client-side exploitation takes place.

Let's dissect the campaign, expose the malicious portfolio of domains involved in it, provide MD5s of the served

malware as well as a sample exploit, and provide actionable (historical) intelligence regarding related malicious

activities that have been taking place using same infrastructure that's involved in the Pinterest campaign.

Spamvertised malicious URL:

boxenteam.com/hathaway/index.html?emailmpss/PSEUDO_RANDOM_CHARACTERS

Attempts to load the following malicious scripts:

theodoxos.gr/hairstyles/defiling.js

web29.webbox11.server-home.org/volleyballs/cloture.js

knopflos-combo.de/subdued/opposition.js

Sample client-side exploits serving URL:

pizzapluswindsor.ca/topic/latest-blog-news.php

Malicious domain name reconnaissance:

pizzapluswindsor.ca - 50.116.6.57; 174.140.169.145

722

Responding to the same IP (50.116.6.57) are also the following malicious domains part of the campaign's infrastructure:

pizzapluswindsor.ca

plainidea.com

procreature.com

poindextersonpatrol.com

pixieglitztutus.com

Known to have responded to the second IP (174.140.169.145) are also the following malicious

domains:

lesperancerenovations.com

louievozza.com

louvozza.com

lv-contracting.com

lvconcordecontracting.com

mcbelectrical.ca

oliviagurun.com

onecable.ca

onlyidea.com

originalpizzaplus.ca

originalpizzaplus.com

papak.ca

pccreature.com

pixieglitztutus.com

pizzapluswindsor.ca

saltlakecityutahcommercialrealestate.com

**The following malicious MD5s are known to have
phoned back to the same IP on the 22nd of
September,**

2013:

MD5: 5d14ee5800fc3c73e4d40567044c4149

MD5: bdc2ac48921914f25d1a3a164266cebc

MD5: a0b2ba75ba7ad7ad5a5b87a966fddb07

MD5: 31c3eae608247c2901d64643d5626b1f

MD5: 3cff9bba085254f2a524207a1388b015

MD5: b59743a3b128c9676548510627db4ac5

MD5: 53004bb63d32792c9bc1b8b26db0f197

MD5: b59743a3b128c9676548510627db4ac5

MD5: 53004bb63d32792c9bc1b8b26db0f197

MD5: 94e7cf26589baac1d47d6834e6375a62

MD5: 38461b4537fb269b2142e7fbac16375b

MD5: 041e9ccce8809371b07f0ac1c4d02b33

MD5: 868cf2c7af8863aebbaeb42c1b404b36

MD5: 7ec71f392dfc98336808ca6e31f25969

MD5: 6792b758ea961f58ad5b2f1eb96a648a

MD5: 33550cef428cad48ba776ea109fe1936

MD5: af84138bc55192ce722582def2f05200

MD5: 170524f3457d1fa681cc5dafbcc86199

MD5: e3af059e42b82b8658f3d05043a5a213

MD5: 4724783ae2c928b40dd2c0ac6d85cbc4

MD5: 9b8d87230ee7f553e8a9011a37ca699e

MD5: e4d63169ddac5e34fe000dc21c88682f

723

MD5: 5f777af07c79369310dff97d04c026cd

MD5: 200badc2e35ce57f1e511aea7322e207

MD5: 93fe170f26d99aea52b30b74afdf96bc

MD5: d06a0cc046e99496ada5591d9f457fc1

MD5: 6f857be5377a7543858aacefea6f1a30

MD5: 92ed463b3c38f2c951c3acd78e7a2df3

MD5: 8f01cd5ddd6e599e79ddcefbff9c0891

Detection rate for a sample served exploit from the Pinterest themed campaign:

[1]**MD5:**

d49275523cae83a5e7639bb22604dd86 - detected by 5 out of 48 antivirus scanners as

HEUR:Exploit.Java.CVE-2012-1723.gen

Upon successful client-side exploitation, the campaign drops two malware samples on the affected hosts.

Detection rate for the first dropped sample:

[2]**MD5:**

ae840d6ac2f02b4bff85182d2c72a053 - detected by 6 out of 48 antivirus scanners as

UDS: DangerousObject.Multi.Generic

Once executed, it phones back to the following C &C:

78.140.131.151/uploading/id=REDACTED &u=PSEUDO_RANDOM_CHARACTERS

The following malicious MD5s are also known to have phoned back to the following C &C IP (78.140.131.151) in

the past:

MD5: ca783e0964e7dcb91fcc2a2ff4b8058f

MD5: d02b0e60f94d718fca19893f13dbd93e

MD5: 3618032d05c12e6d25aa4b7bc9086e06

MD5: 20777b8e6362f8775060fc4fdb191978

MD5: 5a1fb639f5dd97b62b5cf79c84d479f6

MD5: 30f8d972566930c103f9edb7f9bd699e

MD5: 7011abeefd5c9e7c21e3cbe28cc5e71a

MD5: bbb57f1a5004b6adc016c0c9e92add19

MD5: cca6b7fae6678c4b17f21b2ed4580404

MD5: 0decc3f58519c587949dff871fccba5e

MD5: 1b18f9138adbd6b4bf7125c7e6a97aae

MD5: 1e4451c19f07ef6bde87ffbcecc5afb3

MD5: e92297e402fcd03f06c94fe52985a3e9

MD5: 818e329757630bccc9536151f533fad2

MD5: 79e8677f857531118e61fa9238287acb

MD5: de8ef966e7e5251b642540e715d673a6

MD5: 9be83dc4b829ffba26029b173b36237d

MD5: c9b3f7888faa393ee14815494a311684

MD5: d90058b75b8730f9d6bf94a845b3dfda

MD5: e14b4290eec92ce6cd3e0349c17bc062

MD5: 6d5f5419f6a116f4283ae58516ff90a1

MD5: d0587b6e83a70798077e2938af66c50c

MD5: 12449febf7efed7bceade5720c8f635d

MD5: 992fc7370b39553ebcb3c03c23c15517

MD5: 1c198a6b80b1dcf280db30133c26d479

MD5: 7bb85f458b6b8a0bc98d47447b44c5b6

MD5: 1a3679c0c7c42781d9ee5b6987efa726

724

MD5: 7d21915fc425b3545c8e156116f91e00

Detection rate for the second dropped sample:

[3]**MD5:**

83bbe52c8584a5dab07a11ecc5aaf090 - detected by 3
out of 48 antivirus scanners as Trojan-

Spy.Win32.Zbot.qgje; Trojan.Backdoor.RV

Once executed it starts listening on ports 7867 and 1653.

The sample then creates the following Mutexes on the affected hosts:

Local\ {B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A }

Local\ {B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A }

Local\ {D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A }

Local\ {D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A }

Local\ {0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A }

Local\ {911F9FCD-AFAC-6AF2-DBC9-BE58FA349D4A }

Global\ {2E06BA86-8AE7-D5EB-DBC9-BE58FA349D4A }

Global\ {B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A }

Global\ {B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A }

Global\ {D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A }

Global\ {D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A }

Global\ {0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A }

Global\ {BB67AFC4-9FA5-408A-DBC9-BE58FA349D4A }

Global\ {EFF344E9-7488-141E-11EB-B06D3016937F }

Global\ {EFF344E9-7488-141E-75EA-B06D5417937F }

Global\ {EFF344E9-7488-141E-4DE9-B06D6C14937F }

Global\ {EFF344E9-7488-141E-65E9-B06D4414937F }
Global\ {EFF344E9-7488-141E-89E9-B06DA814937F }
Global\ {EFF344E9-7488-141E-BDE9-B06D9C14937F }
Global\ {EFF344E9-7488-141E-51E8-B06D7015937F }
Global\ {EFF344E9-7488-141E-81E8-B06DA015937F }
Global\ {EFF344E9-7488-141E-FDE8-B06DDC15937F }
Global\ {EFF344E9-7488-141E-0DEF-B06D2C12937F }
Global\ {EFF344E9-7488-141E-5DEF-B06D7C12937F }
Global\ {EFF344E9-7488-141E-95EE-B06DB413937F }
Global\ {EFF344E9-7488-141E-F1EE-B06DD013937F }
Global\ {EFF344E9-7488-141E-89EB-B06DA816937F }
Global\ {EFF344E9-7488-141E-F9EF-B06DD812937F }
Global\ {EFF344E9-7488-141E-E5EF-B06DC412937F }
Global\ {EFF344E9-7488-141E-0DEE-B06D2C13937F }
Global\ {EFF344E9-7488-141E-09ED-B06D2810937F }
Global\ {EFF344E9-7488-141E-51EF-B06D7012937F }
Global\ {EFF344E9-7488-141E-35EC-B06D1411937F }
Global\ {EFF344E9-7488-141E-55EF-B06D7412937F }
Global\ {DDB39BDC-ABBD-265E-DBC9-BE58FA349D4A }
Global\ {2E1C200D-106C-D5F1-DBC9-BE58FA349D4A }

MPSWabDataAccessMutex

MPSWABOIkStoreNotifyMutex

Once

executed,

it

also

drops

MD5:

2da7bbc5677313c2876b571b39edc7cf

and

MD5:

83bbe52c8584a5dab07a11ecc5aaf090 on the affected hosts.

725

It then phones back to the following C &C (command and control servers):

99.157.164.179

174.76.94.24

99.60.68.114

217.35.75.232

184.145.205.63

99.60.111.51

207.47.212.146

108.240.232.212

107.193.222.108

We've already seen (some of) these C &C IPs in the following profiled malicious campaign "[4]**Spamvertised**

Facebook 'You have friend suggestions, friend requests and photo tags' Themed Emails Lead to Client-side Exploits

and Malware".

This post has been reproduced from [5]Dancho Danchev's blog . Follow him [6]on Twitter.

1.

<https://www.virustotal.com/en/file/bd7c0f52fd7d7e9b20ab9e8f13ac114243a4f09433f484f8fbc3b51c7c44650d/analysis/1380650108/>

2.

<https://www.virustotal.com/en/file/2dbc3ad0626cbb577ec319b7a62b07b6899ffa74ad98309a6390623f2cd9cdd2/analysis/1380650448/>

3.

<https://www.virustotal.com/en/file/db9345188d8b913b7abd5ea998f67fb7d4fb7aa054e48c52641e795d9b3c7e28/analysis/1380650677/>

4. <http://ddanchev.blogspot.com/2013/09/spamvertised-facebook-you-have-friend.html>

5. <http://ddanchev.blogspot.com/>

6. <http://twitter.com/danchodanchev>

726



Fake Pinterest 'Don't forget to confirm your email!' Themed Emails Serve Client-side Exploits and Malware (2013-10-01 21:12)

Cybercriminals have just launched yet another massive spam campaign, this time attempting to trick Pinterest users

into thinking that they've received an email confirmation request. In reality though, once users click on the links

found in the malicious emails, they're automatically exposed to client-side exploits, with the campaign dropping two

malware samples on the affected hosts once a successful client-side exploitation takes place.

Let's dissect the campaign, expose the malicious portfolio of domains involved in it, provide MD5s of the served

malware as well as a sample exploit, and provide actionable (historical) intelligence regarding related malicious

activities that have been taking place using same infrastructure that's involved in the Pinterest campaign.

Spamvertised malicious URL:

boxenteam.com/hathaway/index.html?emailmpss/PSEUDO_RANDOM_CHARACTERS

Attempts to load the following malicious scripts:

theodoxos.gr/hairstyles/defiling.js

web29.webbox11.server-home.org/volleyballs/cloture.js

knopflos-combo.de/subdued/opposition.js

Sample client-side exploits serving URL:

pizzapluswindsor.ca/topic/latest-blog-news.php

Malicious domain name reconnaissance:

pizzapluswindsor.ca - 50.116.6.57; 174.140.169.145

727

Responding to the same IP (50.116.6.57) are also the following malicious domains part of the campaign's infrastructure:

pizzapluswindsor.ca

plainidea.com

procreature.com

poindextersonpatrol.com

pixieglitztutus.com

Known to have responded to the second IP (174.140.169.145) are also the following malicious domains:

lesperancerenovations.com

louievozza.com

louvozza.com

lv-contracting.com

lvconcordecontracting.com

mcbelectrical.ca

oliviagurun.com

onecable.ca

onlyidea.com

originalpizzaplus.ca

originalpizzaplus.com

papak.ca

pccreature.com

pixieglitztutus.com

pizzapluswindsor.ca

saltlakecityutahcommercialrealestate.com

**The following malicious MD5s are known to have
phoned back to the same IP on the 22nd of
September,**

2013:

MD5: 5d14ee5800fc3c73e4d40567044c4149

MD5: bdc2ac48921914f25d1a3a164266cebc

MD5: a0b2ba75ba7ad7ad5a5b87a966fddb07

MD5: 31c3eae608247c2901d64643d5626b1f

MD5: 3cff9bba085254f2a524207a1388b015

MD5: b59743a3b128c9676548510627db4ac5

MD5: 53004bb63d32792c9bc1b8b26db0f197

MD5: b59743a3b128c9676548510627db4ac5

MD5: 53004bb63d32792c9bc1b8b26db0f197

MD5: 94e7cf26589baac1d47d6834e6375a62

MD5: 38461b4537fb269b2142e7fbac16375b

MD5: 041e9ccce8809371b07f0ac1c4d02b33

MD5: 868cf2c7af8863aebbaeb42c1b404b36

MD5: 7ec71f392dfc98336808ca6e31f25969

MD5: 6792b758ea961f58ad5b2f1eb96a648a

MD5: 33550cef428cad48ba776ea109fe1936

MD5: af84138bc55192ce722582def2f05200

MD5: 170524f3457d1fa681cc5dafbcc86199

MD5: e3af059e42b82b8658f3d05043a5a213

MD5: 4724783ae2c928b40dd2c0ac6d85cbc4

MD5: 9b8d87230ee7f553e8a9011a37ca699e

MD5: e4d63169ddac5e34fe000dc21c88682f

728

MD5: 5f777af07c79369310dff97d04c026cd

MD5: 200badc2e35ce57f1e511aea7322e207

MD5: 93fe170f26d99aea52b30b74afdf96bc

MD5: d06a0cc046e99496ada5591d9f457fc1

MD5: 6f857be5377a7543858aacefea6f1a30

MD5: 92ed463b3c38f2c951c3acd78e7a2df3

MD5: 8f01cd5ddd6e599e79ddcefbff9c0891

Detection rate for a sample served exploit from the Pinterest themed campaign:

[1]**MD5:**

d49275523cae83a5e7639bb22604dd86 - detected by 5 out of 48 antivirus scanners as

HEUR:Exploit.Java.CVE-2012-1723.gen

Upon successful client-side exploitation, the campaign drops two malware samples on the affected hosts.

Detection rate for the first dropped sample:

[2]**MD5:**

ae840d6ac2f02b4bff85182d2c72a053 - detected by 6 out of 48 antivirus scanners as

UDS:DangerousObject.Multi.Generic

Once executed, it phones back to the following C &C:

*78.140.131.151/uploading/id=REDACTED &u=PSEUDO
_RANDOM_CHARACTERS*

**The following malicious MD5s are also known to have
phoned back to the following C &C IP
(78.140.131.151) in**

the past:

MD5: ca783e0964e7dcb91fcc2a2ff4b8058f

MD5: d02b0e60f94d718fca19893f13dbd93e

MD5: 3618032d05c12e6d25aa4b7bc9086e06

MD5: 20777b8e6362f8775060fc4fdb191978

MD5: 5a1fb639f5dd97b62b5cf79c84d479f6

MD5: 30f8d972566930c103f9edb7f9bd699e

MD5: 7011abeefd5c9e7c21e3cbe28cc5e71a

MD5: bbb57f1a5004b6adc016c0c9e92add19

MD5: cca6b7fae6678c4b17f21b2ed4580404

MD5: 0decc3f58519c587949dff871fccba5e

MD5: 1b18f9138adbd6b4bf7125c7e6a97aae

MD5: 1e4451c19f07ef6bde87ffbbecc5afb3

MD5: e92297e402fcd03f06c94fe52985a3e9

MD5: 818e329757630bccc9536151f533fad2

MD5: 79e8677f857531118e61fa9238287acb

MD5: de8ef966e7e5251b642540e715d673a6

MD5: 9be83dc4b829ffba26029b173b36237d

MD5: c9b3f7888faa393ee14815494a311684

MD5: d90058b75b8730f9d6bf94a845b3dfda

MD5: e14b4290eec92ce6cd3e0349c17bc062

MD5: 6d5f5419f6a116f4283ae58516ff90a1

MD5: d0587b6e83a70798077e2938af66c50c

MD5: 12449febf7efed7bceade5720c8f635d

MD5: 992fc7370b39553ebcb3c03c23c15517

MD5: 1c198a6b80b1dcf280db30133c26d479

MD5: 7bb85f458b6b8a0bc98d47447b44c5b6

MD5: 1a3679c0c7c42781d9ee5b6987efa726

729

MD5: 7d21915fc425b3545c8e156116f91e00

Detection rate for the second dropped sample:

[3]MD5:

83bbe52c8584a5dab07a11ecc5aaf090 - detected by 3
out of 48 antivirus scanners as Trojan-

Spy.Win32.Zbot.qgje; Trojan.Backdoor.RV

Once executed it starts listening on ports 7867 and 1653.

The sample then creates the following Mutexes on the affected hosts:

Local\ {B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A }

Local\ {B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A }

Local\ {D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A }

Local\ {D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A }

Local\ {0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A }

Local\ {911F9FCD-AFAC-6AF2-DBC9-BE58FA349D4A }

Global\ {2E06BA86-8AE7-D5EB-DBC9-BE58FA349D4A }

Global\ {B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A }

Global\ {B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A }

Global\ {D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A }

Global\ {D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A }

Global\ {0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A }

Global\ {BB67AFC4-9FA5-408A-DBC9-BE58FA349D4A }

Global\ {EFF344E9-7488-141E-11EB-B06D3016937F }

Global\ {EFF344E9-7488-141E-75EA-B06D5417937F }

Global\ {EFF344E9-7488-141E-4DE9-B06D6C14937F }

Global\ {EFF344E9-7488-141E-65E9-B06D4414937F }

Global\ {EFF344E9-7488-141E-89E9-B06DA814937F }
Global\ {EFF344E9-7488-141E-BDE9-B06D9C14937F }
Global\ {EFF344E9-7488-141E-51E8-B06D7015937F }
Global\ {EFF344E9-7488-141E-81E8-B06DA015937F }
Global\ {EFF344E9-7488-141E-FDE8-B06DDC15937F }
Global\ {EFF344E9-7488-141E-0DEF-B06D2C12937F }
Global\ {EFF344E9-7488-141E-5DEF-B06D7C12937F }
Global\ {EFF344E9-7488-141E-95EE-B06DB413937F }
Global\ {EFF344E9-7488-141E-F1EE-B06DD013937F }
Global\ {EFF344E9-7488-141E-89EB-B06DA816937F }
Global\ {EFF344E9-7488-141E-F9EF-B06DD812937F }
Global\ {EFF344E9-7488-141E-E5EF-B06DC412937F }
Global\ {EFF344E9-7488-141E-0DEE-B06D2C13937F }
Global\ {EFF344E9-7488-141E-09ED-B06D2810937F }
Global\ {EFF344E9-7488-141E-51EF-B06D7012937F }
Global\ {EFF344E9-7488-141E-35EC-B06D1411937F }
Global\ {EFF344E9-7488-141E-55EF-B06D7412937F }
Global\ {DDB39BDC-ABBD-265E-DBC9-BE58FA349D4A }
Global\ {2E1C200D-106C-D5F1-DBC9-BE58FA349D4A }
MPSWabDataAccessMutex

MPSWABOIkStoreNotifyMutex

Once

executed,

it

also

drops

MD5:

2da7bbc5677313c2876b571b39edc7cf

and

MD5:

83bbe52c8584a5dab07a11ecc5aaf090 on the affected hosts.

730

It then phones back to the following C &C (command and control servers):

99.157.164.179

174.76.94.24

99.60.68.114

217.35.75.232

184.145.205.63

99.60.111.51

207.47.212.146

108.240.232.212

107.193.222.108

We've already seen (some of) these C &C IPs in the following profiled malicious campaign "[4]**Spamvertised**

Facebook 'You have friend suggestions, friend requests and photo tags' Themed Emails Lead to Client-side Exploits

and Malware".

Updates will be posted as soon as new developments take place.

1.
[https://www.virustotal.com/en/file/bd7c0f52fd7d7e9b20ab9e8f13ac114243a4f09433f484f8fbc3b51c7c44650d/analysis](https://www.virustotal.com/en/file/bd7c0f52fd7d7e9b20ab9e8f13ac114243a4f09433f484f8fbc3b51c7c44650d/analysis/1380650108/)

[is/1380650108/](https://www.virustotal.com/en/file/bd7c0f52fd7d7e9b20ab9e8f13ac114243a4f09433f484f8fbc3b51c7c44650d/analysis/1380650108/)

2.
[https://www.virustotal.com/en/file/2dbc3ad0626cbb577ec319b7a62b07b6899ffa74ad98309a6390623f2cd9cdd2/analysis](https://www.virustotal.com/en/file/2dbc3ad0626cbb577ec319b7a62b07b6899ffa74ad98309a6390623f2cd9cdd2/analysis/1380650448/)

[is/1380650448/](https://www.virustotal.com/en/file/2dbc3ad0626cbb577ec319b7a62b07b6899ffa74ad98309a6390623f2cd9cdd2/analysis/1380650448/)

3.
[https://www.virustotal.com/en/file/db9345188d8b913b7abd5ea998f67fb7d4fb7aa054e48c52641e795d9b3c7e28/analysis](https://www.virustotal.com/en/file/db9345188d8b913b7abd5ea998f67fb7d4fb7aa054e48c52641e795d9b3c7e28/analysis/1380650677/)

[is/1380650677/](https://www.virustotal.com/en/file/db9345188d8b913b7abd5ea998f67fb7d4fb7aa054e48c52641e795d9b3c7e28/analysis/1380650677/)

4. <http://ddanchev.blogspot.com/2013/09/spamvertised-facebook-you-have-friend.html>

731



Summarizing Webroot's Threat Blog Posts for September (2013-10-02 16:10)

The following is a brief summary of all of my posts at [1]**Webroot's Threat Blog** for September, 2013. You can

subscribe to [2]**Webroot's Threat Blog RSS Feed**, or follow me on Twitter:

- 01.** [3]DIY malicious Android APK generating 'sensitive information stealer' spotted in the wild
- 02.** [4]Scammers pop up in Android's Calendar App
- 03.** [5]Web-based DNS amplification DDoS attack mode supporting PHP script spotted in the wild
- 04.** [6]Managed Malicious Java Applets Hosting Service Spotted in the Wild
- 05.** [7]Affiliate network for mobile malware impersonates Google Play, tricks users into installing premium-rate SMS sending rogue apps
- 06.** [8]419 advance fee fraudsters abuse CNN's 'Email This' Feature, spread Syrian Crisis themed scams
- 07.** [9]Cybercriminals offer anonymous mobile numbers for 'SMS activation', video tape the destruction of the SIM card on request

08. [10]Yet another 'malware-infected hosts as anonymization stepping stones' service offering access to hundreds of compromised hosts spotted in the wild

09. [11]Cybercriminals experiment with 'Socks4/Socks5/HTTP' malware-infected hosts based DIY DoS tool

10. [12]Cybercriminals sell access to tens of thousands of malware-infected Russian hosts

11. [13]Spamvertised "FDIC: Your business account" themed emails serve client-side exploits and malware

12. [14]Cybercriminals experiment with Android compatible, Python-based SQL injecting releases

13. [15]Newly launched E-shop offers access to hundreds of thousands of compromised accounts

14. [16]DIY commercial CAPTCHA-solving automatic email account registration tool available on the underground

market since 2008

15. [17]Yet another subscription-based stealth Bitcoin mining tool spotted in the wild

This post has been reproduced from [18]Dancho Danchev's blog . Follow him [19]on Twitter.

1. <http://www.webroot.com/blog>

2. <http://feeds2.feedburner.com/WebrootThreatBlog>

3. <http://www.webroot.com/blog/2013/09/06/diy-malicious-android-apk-generating-sensitive-information-stealer>

[-spotted-wild/](#)

4. <http://www.webroot.com/blog/2013/09/09/scammers-pop-androids-calendar-app/>

5. <http://www.webroot.com/blog/2013/09/10/web-based-dns-amplification-ddos-attack-mode-supporting-php-script>

[-spotted-wild/](#)

6. <http://www.webroot.com/blog/2013/09/11/managed-malicious-java-applets-hosting-service-spotted-wild/>

7. [http://www.webroot.com/blog/2013/09/18/affiliate-network-mobile-malware-impersonates-google-play-tricks-u](http://www.webroot.com/blog/2013/09/18/affiliate-network-mobile-malware-impersonates-google-play-tricks-users-installing-premium-rate-sms-sending-rogue-apps/)

[sers-installing-premium-rate-sms-sending-rogue-apps/](#)

8.

[http://www.webroot.com/blog/2013/09/18/419-advance-fee-fraudsters-abuse-cnns-email-feature-spread-syrian-](http://www.webroot.com/blog/2013/09/18/419-advance-fee-fraudsters-abuse-cnns-email-feature-spread-syrian-crisis-themed-scams/)

[crisis-themed-scams/](#)

9. [http://www.webroot.com/blog/2013/09/19/cybercriminals-offer-anonymous-mobile-numbers-sms-activation-video](http://www.webroot.com/blog/2013/09/19/cybercriminals-offer-anonymous-mobile-numbers-sms-activation-video-tape-destruction-sim-request/)

[-tape-destruction-sim-request/](#)

10. [http://www.webroot.com/blog/2013/09/20/yet-another-malware-infected-hosts-anonymization-stepping-stones-s](http://www.webroot.com/blog/2013/09/20/yet-another-malware-infected-hosts-anonymization-stepping-stones-service-offering-access-hundreds-compromised-hosts-spott)

[ervice-offering-access-hundreds-compromised-hosts-spott](#)

11.

[http://www.webroot.com/blog/2013/09/20/cybercriminals-release-new-socks4socks5-malware-infected-hosts-bas](http://www.webroot.com/blog/2013/09/20/cybercriminals-release-new-socks4socks5-malware-infected-hosts-based-diy-dos-tool/)

[ed-diy-dos-tool/](http://www.webroot.com/blog/2013/09/20/cybercriminals-release-new-socks4socks5-malware-infected-hosts-based-diy-dos-tool/)

12.

[http://www.webroot.com/blog/2013/09/23/cybercriminals-sell-access-tens-thousands-malware-infected-russian](http://www.webroot.com/blog/2013/09/23/cybercriminals-sell-access-tens-thousands-malware-infected-russian-hosts/)

[-hosts/](http://www.webroot.com/blog/2013/09/23/cybercriminals-sell-access-tens-thousands-malware-infected-russian-hosts/)

13. [http://www.webroot.com/blog/2013/09/23/spamvertised-fdic-business-account-themed-emails-server-client-sid](http://www.webroot.com/blog/2013/09/23/spamvertised-fdic-business-account-themed-emails-server-client-side-exploits-malware/)

[e-exploits-malware/](http://www.webroot.com/blog/2013/09/23/spamvertised-fdic-business-account-themed-emails-server-client-side-exploits-malware/)

14.

[http://www.webroot.com/blog/2013/09/24/cybercriminals-experiment-android-based-sql-injecting-python-based](http://www.webroot.com/blog/2013/09/24/cybercriminals-experiment-android-based-sql-injecting-python-based-releases/)

[-releases/](http://www.webroot.com/blog/2013/09/24/cybercriminals-experiment-android-based-sql-injecting-python-based-releases/)

15. [http://www.webroot.com/blog/2013/09/25/newly-launched-e-shop-offers-access-hundreds-thousands-compromised](http://www.webroot.com/blog/2013/09/25/newly-launched-e-shop-offers-access-hundreds-thousands-compromised-accounts/)

[-accounts/](http://www.webroot.com/blog/2013/09/25/newly-launched-e-shop-offers-access-hundreds-thousands-compromised-accounts/)

16. [http://www.webroot.com/blog/2013/09/27/diy-commercial-captcha-solving-automatic-email-account-registratio](http://www.webroot.com/blog/2013/09/27/diy-commercial-captcha-solving-automatic-email-account-registration-tool-available-underground-market-since-2008/)

[n-tool-available-underground-market-since-2008/](http://www.webroot.com/blog/2013/09/27/diy-commercial-captcha-solving-automatic-email-account-registration-tool-available-underground-market-since-2008/)

17. http://www.webroot.com/blog/2013/09/27/another-subscription-based-stealth-bitcoin-mining-tool-spotted

[-wild/](#)

18. <http://ddanchev.blogspot.com/>

19. <http://twitter.com/danchodanchev>

733

1.11

November

734



Summarizing Webroot's Threat Blog Posts for October (2013-11-01 17:54)

The following is a brief summary of all of my posts at [1]**Webroot's Threat Blog** for October, 2013. You can subscribe to [2]**Webroot's Threat Blog RSS Feed**, or follow me on Twitter:

01. [3]A peek inside a Blackhat SEO/cybercrime-friendly doorways management platform

02. [4]Newly launched 'HTTP-based botnet setup as a service' empowers novice cybercriminals with bulletproof

hosting capabilities - part two

03. [5]'T-Mobile MMS message has arrived' themed emails lead to malware

04. [6]DDoS for hire vendor 'vertically integrates' starts offering TDoS attack capabilities

05. [7]Commercially available Blackhat SEO enabled multi-third-party product licenses empowered VPSs spotted in the wild

06. [8]New cybercrime-friendly iFrames-based E-shop for traffic spotted in the wild

07. [9]Cybercriminals offer spam-friendly SMTP servers for rent – part two

08. [10]Newly launched VDS-based cybercrime-friendly hosting provider helps facilitate fraudulent/malicious online activity

09. [11]Fake ‘You have missed emails’ GMail themed emails lead to pharmaceutical scams

10. [12]Compromised Turkish Government Web site leads to malware

11. [13]Novice cybercriminals offer commercial access to five mini botnets

12. [14]Spamadvertised T-Mobile ‘Picture ID Type:MMS’ themed emails lead to malware

13. [15]Yet another Bitcoin accepting E-shop offering access to thousands of hacked PCs spotted in the wild

14. [16]Malicious ‘FW: File’ themed emails lead to malware

15. [17]Mass iframe injection campaign leads to Adobe Flash exploits

16. [18]Rogue ads lead to the ‘Mipony Download Accelerator/FunMoods Toolbar’ PUA (Potentially Unwanted

Application)

17. [19]A peek inside the administration panel of a standardized E-shop for compromised accounts

18. [20]U.K users targeted with fake 'Confirming your Sky offer' malware serving emails

19. [21]New DIY compromised hosts/proxies syndicating tool spotted in the wild

735

20. [22]Rogue ads lead to the 'EzDownloaderpro' PUA (Potentially Unwanted Application)

21. [23]Fake 'Scanned Image from a Xerox WorkCentre' themed emails lead to malware

22. [24]Fake 'Important: Company Reports' themed emails lead to malware

23. [25]Cybercriminals release new commercially available Android/BlackBerry supporting mobile malware bot

24. [26]Fake WhatsApp 'Voice Message Notification/1 New Voicemail' themed emails lead to malware

This post has been reproduced from [27]Dancho Danchev's blog . Follow him [28]on Twitter.

1. <http://www.webroot.com/blog>

2. <http://feeds2.feedburner.com/WebrootThreatBlog>

3. <http://www.webroot.com/blog/2013/10/01/peek-inside-blackhat-seo-friendly-doorways-management-platform/>

4. <http://www.webroot.com/blog/2013/10/01/newly-launched-http-based-botnet-setup-service-empowers-novice-cybercriminals-bulletproof-hosting-capabilities-part-two/>
5. <http://www.webroot.com/blog/2013/10/02/t-mobile-mms-message-arrived-themed-emails-lead-malware/>
6. <http://www.webroot.com/blog/2013/10/03/vertically-integrating-ddos-hire-vendor-spotted-wild/>
7. <http://www.webroot.com/blog/2013/10/04/commercially-available-blackhat-seo-enabled-multi-third-party-bhseo-product-licenses-empowered-vps-servers-spotted-wild/>
8. <http://www.webroot.com/blog/2013/10/04/new-cybercrime-friendly-iframes-based-e-shop-traffic-spotted-wild/>
9. <http://www.webroot.com/blog/2013/10/07/cybercriminals-offer-spam-friendly-smtp-servers-rent-part-two/>
10. <http://www.webroot.com/blog/2013/10/08/newly-launched-vds-based-cybercrime-friendly-hosting-provider-help-s-facilitate-fraudulent-malicious-online-activity/>
11. <http://www.webroot.com/blog/2013/10/09/fake-4-missed-emails-gmail-themed-emails-lead-pharmaceutical-scams/>
12. <http://www.webroot.com/blog/2013/10/10/compromised-turkish-government-web-site-leads-malware/>

13. <http://www.webroot.com/blog/2013/10/11/novice-cybercriminals-offer-commercial-access-5-mini-botnets/>
14. <http://www.webroot.com/blog/2013/10/14/spamvertised-t-mobile-picture-id-typemms-themed-emails-lead-malware/>
15. <http://www.webroot.com/blog/2013/10/16/yet-another-bitcoin-accepting-e-shop-offering-access-thousands-hacked-pcs-spotted-wild/>
16. <http://www.webroot.com/blog/2013/10/16/malicious-fw-file-themed-emails-lead-malware/>
17. <http://www.webroot.com/blog/2013/10/17/mass-iframe-injection-campaign-leads-adobe-flash-exploits/>
18. <http://www.webroot.com/blog/2013/10/18/rogue-ads-lead-mipony-download-accelerator-fun-moods-toolbar-pua-potentially-unwanted-application/>
19. <http://www.webroot.com/blog/2013/10/18/peek-inside-administration-panel-standardized-e-shop-compromised-accounts/>
20. <http://www.webroot.com/blog/2013/10/21/u-k-users-targeted-fake-confirming-sky-offer-themed-malware-serving-emails/>
21. <http://www.webroot.com/blog/2013/10/21/new-diy-compromised-hostsproxies-syndicating-tool-spotted-wild/>

22. <http://www.webroot.com/blog/2013/10/22/rogue-ads-lead-ezdownloaderpro-pua-potentially-unwanted-application/>

23. <http://www.webroot.com/blog/2013/10/22/fake-scanned-image-xerox-workcentre-themed-emails-lead-malware/>

24. <http://www.webroot.com/blog/2013/10/24/fake-important-company-reports-themed-emails-lead-malware/>

25. <http://www.webroot.com/blog/2013/10/25/cybercriminals-release-new-commercially-available-androidblackberry-supporting-mobile-malware-bot/>

26. <http://www.webroot.com/blog/2013/10/28/fake-whatsapp-voice-message-notification1-new-voicemail-themed-emails-lead-malware-2/>

27. <http://ddanchev.blogspot.com/>

28. <http://twitter.com/danchodanchev>

736



Malicious Script Artifacts at China Green Dot Gov Dot Cn - A Reminiscence of Asprox's Multi-Tasking

Activities (2013-11-04 18:33)

Malware artifacts, [1]**abandoned mass** iframe
[2]**embedded/injected campaigns**, and low Quality Assurance (QA)

campaigns, continue popping up on everyone's radar, raising eyebrows as to the extent of incompetence, possible

evasive tactics, plain simple lack of applied QA when maintaining these campaigns, or the end of a campaign's life cycle.

What's the value of assessing such a non-active campaign? Can the analysis provide any clues into related cur-

rently active malicious campaigns that typically for such type of campaigns, continue relying on the same malicious

infrastructure? But of course.

Let's assess the malicious artifacts at **hxxp://chinagreen.gov.cn**, connect them to the multi-tasking activities

conducted on behalf of the Asprox botnet, as well as several spamvertised malware campaigns circa 2010, and

most importantly provide actionable intelligence on currently active campaigns that continue using the very same

infrastructure for command and control purposes.

Malicious scripts at China Green Dot Gov Dot CN:

update.webserviceftp.ru/js.js - seen in "[3]**Dissecting the Xerox WorkCentre Pro Scanned Document Themed Campaign**"

gdi.webserviceftp.ru/js.js - seen in "[4]**Dissecting the Xerox WorkCentre Pro Scanned Document Themed Campaign**"

ver.webserivcekota.ru/js.js - seen in "[5]**Dissecting the Xerox WorkCentre Pro Scanned Document Themed Cam-**

paign"

batch.webserviceaan.ru/js.js - seen in "[6]**Dissecting the Xerox WorkCentre Pro Scanned Document Themed**

Campaign"

nemohuildiin.ru/tds/go.php?sid=1 - seen in "[7]**Dissecting the Xerox WorkCentre Pro Scanned Document Themed Campaign"**

parkperson.ru:8080/index.php?pid=13 - seen in "[8]**Spamvertised Best Buy, Macy's, Evite and Target Themed**

Scareware/Exploits Serving Campaign"

nutcountry.ru:8080/index.php?pid=13 - seen in "[9]**Spamvertised Best Buy, Macy's, Evite and Target Themed**

Scareware/Exploits Serving Campaign"

What's so special about the spamvertised XeroxWorkCentre Pro campaign is that, back in 2010, it used to

drop an Asprox sample, naturally phoning back to well known Asprox C &Cs at the time.

nemohuildiin.ru is known to have responded to 31.31.204.61 and most recently to 5.63.152.19

Known to have responded to the same IP (31.31.204.61) are also the following malicious

domains:

000sstd.com

02143.ru

03111991.ru

0414.ru

0424.ru

050175.ru

054ru.ru

737

06140.ru

0664346910.ru

0801.ru

08108.ru

087474.ru

08755.ru

0925.ru

0go.ru

1-androds.ru

10000taxi.ru

1001domains.ru

100yss.ru

124k.ru

Moreover, we also got a decent number of malicious MD5s known to have used the same IP as C &C over the

last couple of months, indicating that the artifact is still part of the C &C infrastructure of active campaigns.

The following malicious MD5s are also known to have phoned back to the same IP over the last couple of months:

MD5: 3e3d249c43950ac8bedb937f1ea347f5

MD5: 398b5f0c4b8f9adb1db8420801b52562

MD5: 9a1602a2693ae510339ef5f0d25be0b3

MD5: 9bc423773de47d95de1718173ec8485f

MD5: 637db36286b3e300c37e99a0b4772548

MD5: 9829c64613909fbb13fc402f23baff1b

MD5: f23562bafd94f7b836633f1fb7f9e18f

MD5: 7d263c93829447b2399c2e981d66c9df

MD5: 6ee37ead84906711cb2eed6d7f2fcc88

MD5: 54eb099176e7d65817d1b9789845ee4e

MD5: 723618efbd0d3627da09a770e5fd28c2

MD5: 151030c819209af9b7b2ecf2f5c31aa0

MD5: 279d390b9116f0f8ac80321e5fa43453

MD5: f78ff547ce388a403f5ba979025cd556

MD5: afa7090479ac49a3547931fe249c52e3

MD5: a2565684ae4c0af5a99214da83664927

MD5: ce4f032a3e478f4d4cac959b2e999b5a

Known to have responded to 5.63.152.19 are also the following malicious domains:

6tn.ru

azosi.ru

bi-news.ru

buygroup.ru

dnpsirius.ru

enterplus.ru

nemohuildiin.ru

nfs-worlds.ru

rassylka-na-doski.ru

santehnikaoptom.ru

v-odnoklassniki.ru

738

In a cybercrime ecosystem dominated by leaked [10]**DIY mass Web site hacking tools**, and [11]**sophisticated**

iframe-ing platforms, malicious artifacts are a great reminder that as long as the Web site remains susceptible to remote exploitation, it's only a matter of time before a potential cybercriminal embeds/injects malicious script on it. That's cybercrime-friendly common sense.

This post has been reproduced from [12]Dancho Danchev's blog . Follow him [13]on Twitter.

1. <http://www.webroot.com/blog/2012/11/26/cybercriminals-release-stealthy-diy-mass-iframe-injecting-apache-2-modules/>
2. <http://www.webroot.com/blog/2013/06/03/compromised-ftpssh-account-privilege-escalating-mass-iframe-embedding-platform-released-on-the-underground-marketplace/>
3. <http://ddanchev.blogspot.com/2010/07/dissecting-xerox-workcentre-pro-scanned.html>
4. <http://ddanchev.blogspot.com/2010/07/dissecting-xerox-workcentre-pro-scanned.html>
5. <http://ddanchev.blogspot.com/2010/07/dissecting-xerox-workcentre-pro-scanned.html>
6. <http://ddanchev.blogspot.com/2010/07/dissecting-xerox-workcentre-pro-scanned.html>
7. <http://ddanchev.blogspot.com/2010/07/dissecting-xerox-workcentre-pro-scanned.html>
8. <http://ddanchev.blogspot.com/2010/08/spamvertised-best-buy-macys-evite-and.html>

9. <http://ddanchev.blogspot.com/2010/08/spamvertised-best-buy-macys-evite-and.html>
10. <http://www.webroot.com/blog/2013/11/01/peek-inside-google-dorks-based-mass-sql-injecting-tool/>
11. <http://www.webroot.com/blog/2013/06/03/compromised-ftpssh-account-privilege-escalating-mass-iframe-embedding-platform-released-on-the-underground-marketplace/>
12. <http://ddanchev.blogspot.com/>
13. <http://twitter.com/danchodanchev>

739



Malicious Script Artifacts at China Green Dot Gov Dot Cn - A Reminiscence of Asprox's Multi-Tasking

Activities (2013-11-04 18:33)

Malware artifacts, [1]**abandoned mass** iframe
[2]**embedded/injected campaigns**, and low Quality Assurance (QA)

campaigns, continue popping up on everyone's radar, raising eyebrows as to the extend of incompetence, possible

evasive tactics, plain simple lack of applied QA when maintaining these campaigns, or the end of a campaign's life cycle.

What's the value of assessing such a non-active campaign?
Can the analysis provide any clues into related cur-

rently active malicious campaigns that typically for such type of campaigns, continue relying on the same malicious

infrastructure? But of course.

Let's assess the malicious artifacts at **hxxp://chinagreen.gov.cn**, connect them to the multi-tasking activities

conducted on behalf of the Asprox botnet, as well as several spamvertised malware campaigns circa 2010, and

most importantly provide actionable intelligence on currently active campaigns that continue using the very same

infrastructure for command and control purposes.

Malicious scripts at China Green Dot Gov Dot CN:

update.webserviceftp.ru/js.js - seen in "[3]**Dissecting the Xerox WorkCentre Pro Scanned Document Themed**

Campaign"

gdi.webserviceftp.ru/js.js - seen in "[4]**Dissecting the Xerox WorkCentre Pro Scanned Document Themed Campaign"**

ver.webserivcekota.ru/js.js - seen in "[5]**Dissecting the Xerox WorkCentre Pro Scanned Document Themed Cam-**

paign"

batch.webserviceaan.ru/js.js - seen in "[6]**Dissecting the Xerox WorkCentre Pro Scanned Document Themed**

Campaign"

nemohuildiin.ru/tds/go.php?sid=1 - seen in "[7]**Dissecting the Xerox WorkCentre Pro Scanned Document Themed Campaign**"

parkperson.ru:8080/index.php?pid=13 - seen in "[8]**Spamvertised Best Buy, Macy's, Evite and Target Themed**

Scareware/Exploits Serving Campaign"

nutcountry.ru:8080/index.php?pid=13 - seen in "[9]**Spamvertised Best Buy, Macy's, Evite and Target Themed**

Scareware/Exploits Serving Campaign"

What's so special about the spamvertised XeroxWorkCentre Pro campaign is that, back in 2010, it used to

drop an Asprox sample, naturally phoning back to well known Asprox C &Cs at the time.

nemohuildiin.ru is known to have responded to 31.31.204.61 and most recently to 5.63.152.19

Known to have responded to the same IP (31.31.204.61) are also the following malicious domains:

000sstd.com

02143.ru

03111991.ru

0414.ru

0424.ru

050175.ru

054ru.ru

740

06140.ru

0664346910.ru

0801.ru

08108.ru

087474.ru

08755.ru

0925.ru

0go.ru

1-androds.ru

10000taxi.ru

1001domains.ru

100yss.ru

124k.ru

Moreover, we also got a decent number of malicious MD5s known to have used the same IP as C &C over the

last couple of months, indicating that the artifact is still part of the C &C infrastructure of active campaigns.

The following malicious MD5s are also known to have phoned back to the same IP over the last couple of months:

MD5: 3e3d249c43950ac8bedb937f1ea347f5

MD5: 398b5f0c4b8f9adb1db8420801b52562

MD5: 9a1602a2693ae510339ef5f0d25be0b3

MD5: 9bc423773de47d95de1718173ec8485f

MD5: 637db36286b3e300c37e99a0b4772548

MD5: 9829c64613909fbb13fc402f23baff1b

MD5: f23562bafd94f7b836633f1fb7f9e18f

MD5: 7d263c93829447b2399c2e981d66c9df

MD5: 6ee37ead84906711cb2eed6d7f2fcc88

MD5: 54eb099176e7d65817d1b9789845ee4e

MD5: 723618efbd0d3627da09a770e5fd28c2

MD5: 151030c819209af9b7b2ecf2f5c31aa0

MD5: 279d390b9116f0f8ac80321e5fa43453

MD5: f78ff547ce388a403f5ba979025cd556

MD5: afa7090479ac49a3547931fe249c52e3

MD5: a2565684ae4c0af5a99214da83664927

MD5: ce4f032a3e478f4d4cac959b2e999b5a

Known to have responded to 5.63.152.19 are also the following malicious domains:

6tn.ru

azosi.ru

bi-news.ru

buygroup.ru

dnpsirius.ru

enterplus.ru

nemohuildiin.ru

nfs-worlds.ru

rassylka-na-doski.ru

santehnikaoptom.ru

v-odnoklassniki.ru

741

In a cybercrime ecosystem dominated by leaked [10]**DIY mass Web site hacking tools**, and [11]**sophisticated iframe-ing platforms**, malicious artifacts are a great reminder that as long as the Web site remains susceptible to

remote exploitation, it's only a matter of time before a potential cybercriminal embeds/injects malicious script on it.

That's cybercrime-friendly common sense.

Updates will be posted as soon as new developments take place.

1. <http://www.webroot.com/blog/2012/11/26/cybercriminals-release-stealthy-diy-mass-iframe-injecting-apache-2-modules/>

2. <http://www.webroot.com/blog/2013/06/03/compromised-ftpssh-account-privilege-escalating-mass-iframe-embedding-platform-released-on-the-underground-marketplace/>
3. <http://ddanchev.blogspot.com/2010/07/dissecting-xerox-workcentre-pro-scanned.html>
4. <http://ddanchev.blogspot.com/2010/07/dissecting-xerox-workcentre-pro-scanned.html>
5. <http://ddanchev.blogspot.com/2010/07/dissecting-xerox-workcentre-pro-scanned.html>
6. <http://ddanchev.blogspot.com/2010/07/dissecting-xerox-workcentre-pro-scanned.html>
7. <http://ddanchev.blogspot.com/2010/07/dissecting-xerox-workcentre-pro-scanned.html>
8. <http://ddanchev.blogspot.com/2010/08/spamvertised-best-buy-macys-evite-and.html>
9. <http://ddanchev.blogspot.com/2010/08/spamvertised-best-buy-macys-evite-and.html>
10. <http://www.webroot.com/blog/2013/11/01/peek-inside-google-dorks-based-mass-sql-injecting-tool/>
11. <http://www.webroot.com/blog/2013/06/03/compromised-ftpssh-account-privilege-escalating-mass-iframe-embedding-platform-released-on-the-underground-marketplace/>



Scareware, Blackhat SEO, Spam and Google Groups Abuse, Courtesy of the Koobface Gang

(2013-11-04 18:36)

The Koobface gang is known to have embraced the potential of the "underground multi-tasking" model a long

time ago, in order to achieve the "malicious economies of scale" effect. This "underground multi-tasking" most commonly comes in the form of multiple monetization campaigns, which upon closer analysis always lead back to the

Koobface gang's infrastructure. In fact, the gang is so obsessed with efficiency, that particular redirectors and key ma-

licious domains for a particular campaign, are also, simultaneously rotated across all the campaigns that they manage.

For instance, throughout the past half an year, a huge percentage of the malicious infrastructure used simulta-

neously in multiple campaigns, was parked on the [1]now shut down Riccom LTD - AS29550. From the [2]massive

blackhat SEO campaigns affecting millions of legitimate web sites managed by the gang, to the [3]malvertising attack

at the New York Times web site, and [4]the click-fraud facilitating [5]Bahama botnet, the Koobface botnet is only the

tip of the iceberg for the efficient and fraudulent money machine that the gang operates.

743



In this analysis, I'll once again establish a connection between the ongoing blackhat SEO campaigns managed by the

gang (*[6]Blackhat SEO Campaign Hijacks U.S Federal Form Keywords, Serves Scareware; [7]U.S Federal Forms Blackhat SEO Themed Scareware Campaign Expanding; [8]Dissecting the Ongoing U.S Federal Forms Themed Blackhat SEO*

Campaign), with a spam campaign that's also syndicated across multiple Google Groups, and the Koobface botnet

itself, with a particular emphasis on the scareware monetization taking place across all the campaigns.

Related Koobface research and analysis:

[9]The Koobface Gang Wishes the Industry "Happy Holidays"

[10]Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline

[11]Koobface Botnet Starts Serving Client-Side Exploits

[12]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[13]Koobface Botnet's Scareware Business Model - Part Two

[14]Koobface Botnet's Scareware Business Model - Part One

[15]Koobface Botnet Redirects Facebook's IP Space to my Blog

[16]New Koobface campaign spoofs Adobe's Flash updater

[17]Social engineering tactics of the Koobface botnet

[18]Koobface Botnet Dissected in a TrendMicro Report

[19]Movement on the Koobface Front - Part Two

744

[20]Movement on the Koobface Front

[21]Koobface - Come Out, Come Out, Wherever You Are

[22]Dissecting Koobface Worm's Twitter Campaign

This post has been reproduced from [23]Dancho Danchev's blog.

1. <http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html>

2. <http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html>

3. <http://ddanchev.blogspot.com/2009/09/ukrainian-fan-club-features.html>

4. <http://blogs.zdnet.com/security/?p=4549>

5. <http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html>

6. <http://ddanchev.blogspot.com/2009/08/blackhat-seo-campaign-hijacks-us.html>
7. <http://ddanchev.blogspot.com/2009/08/us-federal-forms-blackhat-seo-themed.html>
8. <http://ddanchev.blogspot.com/2009/08/dissecting-ongoing-us-federal-forms.html>
9. <http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html>
10. <http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html>
11. <http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html>
12. <http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html>
13. <http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html>
14. <http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html>
15. <http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html>
16. <http://blogs.zdnet.com/security/?p=4594>
17. http://content.zdnet.com/2346-12691_22-352597.html
18. <http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html>

19. <http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html>
20. <http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html>
21. <http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-whenever-you.html>
22. <http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html>
23. <http://ddanchev.blogspot.com/>

745

Facebook FarmTown Malvertising Campaign Courtesy of the Koobface Gang (2013-11-04 18:36)

Earlier this week, another malvertising campaign affected a popular community, in the face of Facebook's FarmTown.

You have to analyze, and cross-check it to believe it.

Key summary points:

- the email test@now.net.cn used to register all the domains involved in the malvertising campaign, is exclusively

used by the Koobface gang for numerous scareware registrations seen -

a

746

Money Mule Recruiters Trick Mules Into Installing Fake Transaction Certificates (2013-11-04 18:37)

What is more flattering than Ukrainian blackhat SEO gangs using name as redirectors, including offensive messages, the Koobface gang redirecting Facebook's IP space to your blog, or a plain simple danchodanchev admin panel within a Crime Pack kit?

It's the money mule recruiters who modify the HOSTS file of gullible mules to redirect **ddanchev.blogspot.com** and

bobbear.co.uk to 127.0.0.1. Now that's flattering, considering the fact that my public money mule ecosystem related research represents a tiny percentage of the real profiling/activities taking place behind the curtains.

a

Related coverage of money laundering/recruitment in the context of cybercrime:

[1]Keeping Money Mule Recruiters on a Short Leash - Part Four

[2]Money Mule Recruitment Campaign Serving Client-Side Exploits

[3]Keeping Money Mule Recruiters on a Short Leash - Part Three

[4]Money Mule Recruiters on Yahoo!'s Web Hosting

[5]Dissecting an Ongoing Money Mule Recruitment Campaign

[6]Keeping Money Mule Recruiters on a Short Leash - Part Two

[7]Keeping Reshipping Mule Recruiters on a Short Leash

[8]Keeping Money Mule Recruiters on a Short Leash

[9]Standardizing the Money Mule Recruitment Process

[10]Inside a Money Laundering Group's Spamming Operations

[11]Money Mule Recruiters use ASProx's Fast Fluxing Services

[12]Money Mules Syndicate Actively Recruiting Since 2002

This post has been reproduced from [13]Dancho Danchev's blog. Follow him [14]on Twitter.

1. <http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html>

2. <http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html>

3. <http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html>

4. <http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html>

5. <http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html>

6. <http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html>

7. <http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html>

8. <http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html>
9. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>
10. <http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html>
11. <http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asprox-fast.html>
12. <http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html>
13. <http://ddanchev.blogspot.com/>
14. <http://twitter.com/danchodanchev>

747



A Peek Inside a Customer-ized API-enabled DIY Online Lab for Generating Multi-OS Mobile Malware (2013-11-12 02:57)

The exponential growth of mobile malware over the last couple of years, can be attributed to a variety of 'growth factors', the majority of which continue playing an inseparable role in the overall success and growth of the cybercrime ecosystem in general.

Tactics like [1]**standardization**, efficiency-oriented monetization, systematic bypassing of industry

accepted/massively adopted security measures like signatures-based antivirus scanning, [2]**affiliate networks** helping cybercriminals

secure revenue streams for their malicious/fraudulent tactics, techniques and procedures (TTPs), as well as pseudo

legal distribution of deceptive software – think scaware with long EULAs and ToS-es – as well as mobile applications

– think [3]**subscription based premium rate SMS malware** with long EULAs and ToS-es – continue dominating the

arsenal of tactics that any cybercriminal aspiring to occupy a market share in any market segment within the

cybercrime ecosystem, can easily take advantage of in 2013.

What has changed over the last couple of years, in terms of concepts? A lot. For instance, back in 2007, ap-

proximately one year after I (publicly) anticipated the upcoming and inevitable [4]**monetization of mobile malware**,

the Red Browser started making its rounds, proving that I was sadly wrong, and once again, money and greed –

or plain simple profit maximization to others – would play a crucial role in this emerging back then, cybercrime

ecosystem market segment for mobile malware. [5]**Similar monetization attempts** on behalf of cybercriminals, then

followed, to further strengthen the ambitions of cybercriminals into this emerging market segment.

With "[6]**malicious economies of scale**" just starting to materialize at the time, it didn't take long before the concept started getting embedded into virtually each and every cybercrime-friendly product/service advertised

on the market. Thanks to [7]**Symbian OS** dominating the mobile operating system at the time, opportunistic

cybercriminals quickly adapted to steal a piece of the pie, by releasing multiple [8]**Symbian based malware variants**.

Sharing is caring, therefore, here are some MD5s from the Symbian malicious code that used to dominate the threat

landscape, back then.

Symbian OS malware MD5s from that period of time, for historical OSINT purposes:

MD5: a4a70d9c3dbe955dd88ea6975dd909d8

MD5: 98f7cfd42df4a01e2c4f2ed6d38c1af1

MD5: 6fd6b68ed3a83b2850fe293c6db8d78d

MD5: 38837c60e2d87991c6c754f8a6fb5c2d

MD5: ace9c6c91847b29aefa0a50d3b54bac5

MD5: 3f1828f58d676d874a3473c1cd01a431

MD5: 2163ef88da9bd31f471087a55f49d1b1

MD5: 0a04f6fed68dec7507d7bf246aa265eb

MD5: ad4a9c68f631d257bd76490029227e41

MD5: 7a4639488b4698f131e42de56ceeb45d

MD5: fa3de591d3a7353080b724a294dca394
748

MD5: 5ba5fad8923531784cd06a1edc6e0001

MD5: 66abbd9a965b2213f895e297f40552e5

MD5: 92b069ef1fd9a5d9c78a2d3682c16b8f

MD5: a494da11f47a853308bfdb3c0705f4e1

MD5: 9f38eff6c58667880d1ff9feb9093dcb

MD5: a8a3ac5f7639d82b24e9eb4f9ec5981c

MD5: 0ebc8e9f5ec72a0ff73a73d81dc6807d

MD5: a3cd8f8302a69e786425e51467ad5f7c

MD5: 38837c60e2d87991c6c754f8a6fb5c2d

MD5: 522a8efdc382b38e336d4735a73e6b23

MD5: 052abb9b41f07192e8a02f0746e80280

MD5: 712a1184c5fc1811192cba5cc7feda51

MD5: bdae8a51d4f12762b823e42aa6c3fa0a

MD5: aec4b95aa8d80ee9a57d11cb16ce75ba

MD5: 6b854f2171cca50f49d1ace2d454065a

MD5: 945279ce239d2370e4a65b4f109b533b

MD5: cde433d371228fb7310849c03792479e
MD5: 957265e799246225e078a6d65bde5717
MD5: cde433d371228fb7310849c03792479e
MD5: 1f1074b709736fe4504302cbc06fd0f6
MD5: 1cd241a5ea55eb25baf50af25629af27
MD5: 60d9a75b5d3320635f9e33fe76b9b836
MD5: e23f69eea5fa000f259e417b64210d42
MD5: 36503b8a9e2c39508a50eb0bdbb66370
MD5: 1f1074b709736fe4504302cbc06fd0f6
MD5: da13e08a8778fa4ea1d60e8b126e27be
MD5: 642495185b4b22d97869007fcbc0e00f
MD5: 9af5d82f330bbc03f35436b3cc2fba3a
MD5: 6099516a39abb73f9d7f99167157d957
MD5: 6c75b3e9bf4625dc1b754073a2d0c4f1
MD5: e23f69eea5fa000f259e417b64210d42
MD5: ffb37b431ed1f0ac5764b57fa8d4cced
MD5: 1cd241a5ea55eb25baf50af25629af27
MD5: b3055e852b47979a774575c09978981a
MD5: 9f38eff6c58667880d1ff9feb9093dcb
MD5: 945279ce239d2370e4a65b4f109b533b

MD5: 66a0bbebbe14939706093aa5831b53a7

MD5: 30a2797f33ecb66524e01a63e49485dd

MD5: 785e921ea686c2fc8514fac94dd8a9cd

MD5: 69a68bdcbad227d5d8d1a27dd9c30ce7

MD5: f246b101bc66fe36448d0987a36c3e0a

MD5: 4fd086a236c2f3c70b7aa869fa73f762

MD5: 642495185b4b22d97869007fcbc0e00f

MD5: fd8b784df4bbb8082a7534841aa02f0e

MD5: 3ee70d31d0a3b6fab562c51d8ff70e6d

MD5: 3381d21f476d123dcf3b5cbc27b22ae1

MD5: 006b32148ce6747fddb6d89e5725573e

MD5: 7a4639488b4698f131e42de56ceeb45d

MD5: b9667e23bd400edcafde58b61ac05f96

MD5: 12527fd41dd6b172f8e28049011ebd05

749



MD5: c9baecb122bb6d58f765aaca800724d2

MD5: 799531e06e6aa19d569595d32d16f7cc

MD5: e301c2135724db49f4dd5210151e8ae9

MD5: 29d7c73bd737d5bb48f272468a98d673

In 2013, we can easily differentiate between the [9]**botnet building** type of [10]**two-factor authentication by-**

passing mobile trojans, and the ubiquitous for the market segment, subscription based premium rate SMS malware,

relying on deceptive advertising and successful 'visual social engineering' campaigns. The second, continue getting

largely monetized through one of the primary growth factors of the mobile market segment, namely, [11]**affiliate**

networks for mobile malware.

In this post, I'll profile what can be best described as a sophisticated, customer-ized, customization and effi-

ciency oriented, API-supporting, DIY mobile "lab" for generating, managing and operating multi-mobile-operating

systems type of mobile malware campaigns. The service's unique value proposition (UVP) in comparison to that of

competing "labs" for managing, operating and converting mobile traffic - [12]**acquisition and selling** of [13]**mobile traffic** is a commoditized underground market item in 2013 - orbits around the feature rich interface, offering 100

% customization, monitoring and generally operating the campaigns, while efficiently earning fraudulently obtained

revenue from unsuspecting mobile device users.

Sample screenshots featuring the administration panel of an affiliate network participant:

750



751



752



753



754



755



756



757



Sample "system" domains used for hosting/rotating the generated mobile malware samples courtesy of the

service:

jmobl.net - 91.202.63.75

omoby.net - 91.202.63.75

rrmobi.net - 91.202.63.75

moby-aa.ru - 91.202.63.75

mobyc.net - 91.202.63.75

mobi-files.com - 91.202.63.75

mobyw.net - 91.202.63.75

moby.net - 91.202.63.75

mobyc.net - 91.202.63.75

mobyz.net - 91.202.63.75

Known to have responded to the same IP are also the following malicious domains:

doklameno1.ru

doklameno2.ru

758



downloadakpinstall.ru

mobi.net

moby-aa.ru

moby-ae.ru

mobyc.net

mobyw.com

mobyw.net

mobyy.net

mobyz.net

omoby.net

rrmobi.net

system-update.ru

telefontown.pp.ua

Sample Web sites serving multi-mobile-operating-system premium rate mobile malware, relying on the ser-

vice:

759



760



Samples generated and currently distributed in the wild using the service:

[14]**MD5: ac69514f9632539f9e8ad7b944556ed8** -
detected by 15 out of 48 antivirus scanners as HEUR:Trojan-
SMS.AndroidOS.Stealer.a

[15]**MD5: e62f97a095ca15747bb529ee9f1b5057** -
detected by 2 out of 45 antivirus scanners as
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[16]**MD5: 0688dac2754cce01183655bbbe50a0b1** -
detected by 2 out of 46 antivirus scanners as
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[17]**MD5: 4062a77bda6adf6094f4ab209c71b801** -
detected by 2 out of 44 antivirus scanners as
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[18]**MD5: 42a6cf362dbff4fd1b5aa9e82c5b7b56** -
detected by 2 out of 45 antivirus scanners as
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[19]**MD5: 3bcbe78a2fa8c050ee52675d9ec931ad** -
detected by 2 out of 46 antivirus scanners as
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[20]**MD5: 53d3d35cf896938e897de002db6ffc68** -
detected by 2 out of 47 antivirus scanners as
Java.SMSSend.780;

761

J2ME/TrojanSMS.Agent.DX

[21]**MD5: 2f66735b37738017385cc2fb56c21357** -
detected by 2 out of 46 antivirus scanners as
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[22]**MD5: 0ec11bba4a6a86eb5171ecad89d78d05** -
detected by 2 out of 47 antivirus scanners as
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[23]**MD5: 9f059c973637f105271d345a95787a5f** -
detected by 2 out of 45 antivirus scanners as
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[24]**MD5: f179a067580014b1e16900b90d90a872** -
detected by 2 out of 47 antivirus scanners as
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[25]**MD5: aef4f659943cbc530e4e1b601e75b19e** -
detected by 2 out of 46 antivirus scanners as
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[26]**MD5: 8a00786ed6939a8ece2765d503c97ff8** -
detected by 2 out of 45 antivirus scanners as
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[27]**MD5: 868fcf05827c092fa1939930c2f50016** -
detected by 2 out of 45 antivirus scanners as

Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[28]**MD5: a6ef49789845ed1a66f94fd7cc089e1b** -
detected by 2 out of 47 antivirus scanners as
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[29]**MD5: 22aa473772b2dfb0f019dac3b8749bb6** -
detected by 2 out of 45 antivirus scanners as
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[30]**MD5: 52b74046d0c123772566d591524b3bf7** -
detected by 2 out of 46 antivirus scanners as
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[31]**MD5: bfff61a2e3555a6675bc77621be19a73** -
detected by 2 out of 46 antivirus scanners as
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[32]**Cybercrime-friendly affiliate networks** continue,
and will continue to represent a major driving factor be-

hind the growth of any market segment within the
cybercrime system, as they result in a win-win-lose scenario
for

their operations, participants and the potential victims of
the fraudulent/malicious propositions/releases courtesy

of these networks. With mobile traffic acquisition available on demand based on any given preference a potential

could have, cybercriminals would continue converting it into victims, cashing in on their overall lack of awareness of

the TTPs of today's modern cybercriminals.

This post has been reproduced from [33]Dancho Danchev's blog . Follow him [34]on Twitter.

1. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>
2. <http://www.webroot.com/blog/tag/affiliate-networks/>
3. <http://www.webroot.com/blog/2013/09/18/affiliate-network-mobile-malware-impersonates-google-play-tricks-users-installing-premium-rate-sms-sending-rogue-apps/>
4. http://ddanchev.blogspot.com/2007/05/commercializing-mobile-malware_18.html
5. <http://ddanchev.blogspot.com/2008/07/mobile-malware-scam-isexplorer-wants.html>
6. <http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html>
7. <http://www.internetnews.com/wireless/article.php/3584431>
8. <http://ddanchev.blogspot.com/2009/07/transmitterc-mobile-malware-in-wild.html>
- 9.

<http://www.webroot.com/blog/2013/10/25/cybercriminals-release-new-commercially-available-androidblackberry-supporting-mobile-malware-bot/>

[y-supporting-mobile-malware-bot/](http://www.webroot.com/blog/2013/10/25/cybercriminals-release-new-commercially-available-androidblackberry-supporting-mobile-malware-bot/)

10. <http://ddanchev.blogspot.com/2013/07/a-peek-inside-managed-otpatstan-token.html>

11. <http://www.webroot.com/blog/2013/09/18/affiliate-network-mobile-malware-impersonates-google-play-tricks-users-installing-premium-rate-sms-sending-rogue-apps/>

12. <http://www.webroot.com/blog/2013/08/13/cybercrime-friendly-underground-traffic-exchange-helps-facilitate-fraudulent-and-malicious-activity/>

13. <http://www.webroot.com/blog/2013/08/29/cybercrime-friendly-underground-traffic-exchanges-help-facilitate->

[762](http://www.webroot.com/blog/2013/08/29/cybercrime-friendly-underground-traffic-exchanges-help-facilitate-)

[fraudulent-and-malicious-activity-part-two/](http://www.webroot.com/blog/2013/08/29/cybercrime-friendly-underground-traffic-exchanges-help-facilitate-)

14. <https://www.virustotal.com/en/file/1a3e255ccb734021ff8c89b4f14196d065fa1905ab5df398431df4909b1ed1d7/analysis/>

15. <https://www.virustotal.com/en/file/5a0f6fe6d46d6bda81a237d72a60ec55df7062be4dff1abe7712d64d1a6a9a1f/analysis/1383771675/>

16.

[https://www.virustotal.com/en/file/61dd75041770fb177a76658bf620b8568aec47d3c8c779d94913e549090479f8/analysis/](https://www.virustotal.com/en/file/61dd75041770fb177a76658bf620b8568aec47d3c8c779d94913e549090479f8/analysis/1383771784/)

[1383771784/](https://www.virustotal.com/en/file/61dd75041770fb177a76658bf620b8568aec47d3c8c779d94913e549090479f8/analysis/1383771784/)

17.

[https://www.virustotal.com/en/file/195a3be1048d9b8192670a488cf991b39d6ff6c8a3d2996dfef30633fe9eeac5/analysis/](https://www.virustotal.com/en/file/195a3be1048d9b8192670a488cf991b39d6ff6c8a3d2996dfef30633fe9eeac5/analysis/1383771850/)

[1383771850/](https://www.virustotal.com/en/file/195a3be1048d9b8192670a488cf991b39d6ff6c8a3d2996dfef30633fe9eeac5/analysis/1383771850/)

18.

[https://www.virustotal.com/en/file/5c19a007d6620c542940a2ebf441db7a4285ee42cea2e4e4b153aab80b44fa4d/analysis/](https://www.virustotal.com/en/file/5c19a007d6620c542940a2ebf441db7a4285ee42cea2e4e4b153aab80b44fa4d/analysis/1383771922/)

[1383771922/](https://www.virustotal.com/en/file/5c19a007d6620c542940a2ebf441db7a4285ee42cea2e4e4b153aab80b44fa4d/analysis/1383771922/)

19.

[https://www.virustotal.com/en/file/669e7c760993098bfe6f1deb595239ace7809a9674ef5eef0e48631d6743bf04/analysis/](https://www.virustotal.com/en/file/669e7c760993098bfe6f1deb595239ace7809a9674ef5eef0e48631d6743bf04/analysis/1383772019/)

[1383772019/](https://www.virustotal.com/en/file/669e7c760993098bfe6f1deb595239ace7809a9674ef5eef0e48631d6743bf04/analysis/1383772019/)

20.

[https://www.virustotal.com/en/file/0826d6b1d5c803afaec09299e7df3f2763cb39dba91854346fc57d7f610d9299/analysis/](https://www.virustotal.com/en/file/0826d6b1d5c803afaec09299e7df3f2763cb39dba91854346fc57d7f610d9299/analysis/1383772147/)

[1383772147/](https://www.virustotal.com/en/file/0826d6b1d5c803afaec09299e7df3f2763cb39dba91854346fc57d7f610d9299/analysis/1383772147/)

21.

<https://www.virustotal.com/en/file/941bee13931948d2913982efb0d677a2222648ef23893e7cbf773c59bb5ea369/analysis/>

[is/1383772232/](#)

22.

<https://www.virustotal.com/en/file/6cf9503053e927c75a537b2574fa44e203f5fc4079a6446e8b285b13ad8bbf7f/analysis/>

[is/1383772324/](#)

23.

<https://www.virustotal.com/en/file/03734e0e1dc2a834e4892f10cfa52399180cac37579bfd742ea81fa5503e18ff/analysis/>

[is/1383772403/](#)

24.

<https://www.virustotal.com/en/file/f7a8d5bf295dcc0d614ccb10a25aaa7645c9f6c5240da481bf18bbe9f050e8cd/analysis/>

[is/1383783939/](#)

25.

<https://www.virustotal.com/en/file/77779337b988c5c4a606cb5299c0cb92e39766ae05d3cbe5dc005064d1059eb4/analysis/>

[is/1383784127/](#)

26.

<https://www.virustotal.com/en/file/5e9963185d18b01a5900d53f436c70ea4260de9327e52ef97107a755ca60b570/analysis/>

[is/1383784229/](#)

27.

<https://www.virustotal.com/en/file/c618d84e47ef2ccdd11d7a2f3883e5fa7bca52442bf3a0904e1723f3dc459461/analysis/>

[is/1383784294/](#)

28.

<https://www.virustotal.com/en/file/62f4c45a5f698c759e66187d6d322b476e78d973aa6bf6daabcebb2d6139ad2d/analysis>

[is/1383784390/](#)

29.

<https://www.virustotal.com/en/file/26c88732e4895244a937553c25bce2378718fc4e5af0977abdb6cedc9dbb9fbb/analysis>

[is/1383784546/](#)

30.

<https://www.virustotal.com/en/file/0713ef64ca57ab7164142f485208dba9cace1b8f9da3fdaaa0c840541df6b843/analysis>

[is/1383784624/](#)

31.

<https://www.virustotal.com/en/file/f8b10b6ae34c01878d24fd3bf29235b117303dd17b720e15126f0cc6a3110adf/analysis>

[is/1383785064/](#)

32. <http://www.zdnet.com/blog/security/inside-an-affiliate-spam-program-for-pharmaceuticals/2054>

33. <http://ddanchev.blogspot.com/>

34. <http://twitter.com/danchodanchev>

763



A Peek Inside a Customer-ized API-enabled DIY Online Lab for Generating Multi-OS Mobile Malware

(2013-11-12 02:57)

The exponential growth of mobile malware over the last couple of years, can be attributed to a variety of 'growth factors', the majority of which continue playing an inseparable role in the overall success and growth of the cybercrime ecosystem in general.

Tactics like [1]**standardization**, efficiency-oriented monetization, systematic bypassing of industry accepted/massively adopted security measures like signatures-based antivirus scanning, [2]**affiliate networks** helping cybercriminals

secure revenue streams for their malicious/fraudulent tactics, techniques and procedures (TTPs), as well as pseudo

legal distribution of deceptive software – think scaware with long EULAs and ToS-es – as well as mobile applications

– think [3]**subscription based premium rate SMS malware** with long EULAs and ToS-es – continue dominating the

arsenal of tactics that any cybercriminal aspiring to occupy a market share in any market segment within the

cybercrime ecosystem, can easily take advantage of in 2013.

What has changed over the last couple of years, in terms of concepts? A lot. For instance, back in 2007, ap-

proximately one year after I (publicly) anticipated the upcoming and inevitable [4]**monetization of mobile malware**,

the Red Browser started making its rounds, proving that I was sadly wrong, and once again, money and greed –

or plain simple profit maximization to others – would play a crucial role in this emerging back then, cybercrime

ecosystem market segment for mobile malware. [5]**Similar monetization attempts** on behalf of cybercriminals, then

followed, to further strengthen the ambitions of cybercriminals into this emerging market segment.

With "[6]**malicious economies of scale**" just starting to materialize at the time, it didn't take long before the concept started getting embedded into virtually each and every cybercrime-friendly product/service advertised

on the market. Thanks to [7]**Symbian OS** dominating the mobile operating system at the time, opportunistic

cybercriminals quickly adapted to steal a piece of the pie, by releasing multiple [8]**Symbian based malware variants**.

Sharing is caring, therefore, here are some MD5s from the Symbian malicious code that used to dominate the threat

landscape, back then.

Symbian OS malware MD5s from that period of time, for historical OSINT purposes:

MD5: a4a70d9c3dbe955dd88ea6975dd909d8

MD5: 98f7cfd42df4a01e2c4f2ed6d38c1af1

MD5: 6fd6b68ed3a83b2850fe293c6db8d78d

MD5: 38837c60e2d87991c6c754f8a6fb5c2d

MD5: ace9c6c91847b29aefa0a50d3b54bac5

MD5: 3f1828f58d676d874a3473c1cd01a431

MD5: 2163ef88da9bd31f471087a55f49d1b1

MD5: 0a04f6fed68dec7507d7bf246aa265eb

MD5: ad4a9c68f631d257bd76490029227e41

MD5: 7a4639488b4698f131e42de56ceeb45d

MD5: fa3de591d3a7353080b724a294dca394

764

MD5: 5ba5fad8923531784cd06a1edc6e0001

MD5: 66abbd9a965b2213f895e297f40552e5

MD5: 92b069ef1fd9a5d9c78a2d3682c16b8f

MD5: a494da11f47a853308bfdb3c0705f4e1

MD5: 9f38eff6c58667880d1ff9feb9093dcb

MD5: a8a3ac5f7639d82b24e9eb4f9ec5981c

MD5: 0ebc8e9f5ec72a0ff73a73d81dc6807d

MD5: a3cd8f8302a69e786425e51467ad5f7c

MD5: 38837c60e2d87991c6c754f8a6fb5c2d

MD5: 522a8efdc382b38e336d4735a73e6b23

MD5: 052abb9b41f07192e8a02f0746e80280

MD5: 712a1184c5fc1811192cba5cc7feda51

MD5: bdae8a51d4f12762b823e42aa6c3fa0a

MD5: aec4b95aa8d80ee9a57d11cb16ce75ba

MD5: 6b854f2171cca50f49d1ace2d454065a

MD5: 945279ce239d2370e4a65b4f109b533b

MD5: cde433d371228fb7310849c03792479e

MD5: 957265e799246225e078a6d65bde5717

MD5: cde433d371228fb7310849c03792479e

MD5: 1f1074b709736fe4504302cbc06fd0f6

MD5: 1cd241a5ea55eb25baf50af25629af27

MD5: 60d9a75b5d3320635f9e33fe76b9b836

MD5: e23f69eea5fa000f259e417b64210d42

MD5: 36503b8a9e2c39508a50eb0bdbb66370

MD5: 1f1074b709736fe4504302cbc06fd0f6

MD5: da13e08a8778fa4ea1d60e8b126e27be

MD5: 642495185b4b22d97869007fcbc0e00f

MD5: 9af5d82f330bbc03f35436b3cc2fba3a

MD5: 6099516a39abb73f9d7f99167157d957

MD5: 6c75b3e9bf4625dc1b754073a2d0c4f1

MD5: e23f69eea5fa000f259e417b64210d42

MD5: ffb37b431ed1f0ac5764b57fa8d4cced

MD5: 1cd241a5ea55eb25baf50af25629af27

MD5: b3055e852b47979a774575c09978981a

MD5: 9f38eff6c58667880d1ff9feb9093dcb

MD5: 945279ce239d2370e4a65b4f109b533b

MD5: 66a0bbebbe14939706093aa5831b53a7

MD5: 30a2797f33ecb66524e01a63e49485dd

MD5: 785e921ea686c2fc8514fac94dd8a9cd

MD5: 69a68bdcbad227d5d8d1a27dd9c30ce7

MD5: f246b101bc66fe36448d0987a36c3e0a

MD5: 4fd086a236c2f3c70b7aa869fa73f762

MD5: 642495185b4b22d97869007fcbc0e00f

MD5: fd8b784df4bbb8082a7534841aa02f0e

MD5: 3ee70d31d0a3b6fab562c51d8ff70e6d

MD5: 3381d21f476d123dcf3b5cbc27b22ae1

MD5: 006b32148ce6747fddb6d89e5725573e

MD5: 7a4639488b4698f131e42de56ceeb45d

MD5: b9667e23bd400edcafde58b61ac05f96

MD5: 12527fd41dd6b172f8e28049011ebd05

765



MD5: c9baecb122bb6d58f765aaca800724d2

MD5: 799531e06e6aa19d569595d32d16f7cc

MD5: e301c2135724db49f4dd5210151e8ae9

MD5: 29d7c73bd737d5bb48f272468a98d673

In 2013, we can easily differentiate between the [9]**botnet building** type of [10]**two-factor authentication by-**

passing mobile trojans, and the ubiquitous for the market segment, subscription based premium rate SMS malware,

relying on deceptive advertising and successful 'visual social engineering' campaigns. The second, continue getting

largely monetized through one of the primary growth factors of the mobile market segment, namely, [11]**affiliate**

networks for mobile malware.

In this post, I'll profile what can be best described as a sophisticated, customer-ized, customization and effi-

ciency oriented, API-supporting, DIY mobile "lab" for generating, managing and operating multi-mobile-operating

systems type of mobile malware campaigns. The service's unique value proposition (UVP) in comparison to that of

competing "labs" for managing, operating and converting mobile traffic – [12]**acquisition and selling** of [13]**mobile traffic** is a commoditized underground market item in 2013 – orbits around the feature rich interface, offering 100

% customization, monitoring and generally operating the campaigns, while efficiently earning fraudulently obtained revenue from unsuspecting mobile device users.

Sample screenshots featuring the administration panel of an affiliate network participant:

766



767



768



769



770



771



772



773



Sample "system" domains used for hosting/rotating the generated mobile malware samples courtesy of the

service:

jmobi.net - 91.202.63.75

omoby.net - 91.202.63.75

rrmobi.net - 91.202.63.75

moby-aa.ru - 91.202.63.75

mobyc.net - 91.202.63.75

mobi-files.com - 91.202.63.75

mobyw.net - 91.202.63.75

mobyy.net - 91.202.63.75

mobyc.net - 91.202.63.75

mobyz.net - 91.202.63.75

Known to have responded to the same IP are also the following malicious domains:

doklameno1.ru

doklameno2.ru

774



downloadakpinstall.ru

moby.net

moby-aa.ru

moby-ae.ru

moby.com

mobyw.com

mobyw.net

moby.net

moby.net

omoby.net

rrmobi.net

system-update.ru

telefontown.pp.ua

Sample Web sites serving multi-mobile-operating-system premium rate mobile malware, relying on the ser-

vice:

775



776



Samples generated and currently distributed in the wild using the service:

[14]**MD5: ac69514f9632539f9e8ad7b944556ed8** -
detected by 15 out of 48 antivirus scanners as HEUR:Trojan-SMS.AndroidOS.Stealer.a

[15]**MD5: e62f97a095ca15747bb529ee9f1b5057** -
detected by 2 out of 45 antivirus scanners as
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[16]**MD5: 0688dac2754cce01183655bbbe50a0b1** -
detected by 2 out of 46 antivirus scanners as
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[17]**MD5: 4062a77bda6adf6094f4ab209c71b801** -
detected by 2 out of 44 antivirus scanners as
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[18]**MD5: 42a6cf362dbff4fd1b5aa9e82c5b7b56** -
detected by 2 out of 45 antivirus scanners as
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[19]**MD5: 3bcbe78a2fa8c050ee52675d9ec931ad** -
detected by 2 out of 46 antivirus scanners as
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[20]**MD5: 53d3d35cf896938e897de002db6ffc68** -
detected by 2 out of 47 antivirus scanners as
Java.SMSSend.780;

777

J2ME/TrojanSMS.Agent.DX

[21]**MD5: 2f66735b37738017385cc2fb56c21357** -
detected by 2 out of 46 antivirus scanners as
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[22]**MD5: 0ec11bba4a6a86eb5171ecad89d78d05** -
detected by 2 out of 47 antivirus scanners as
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[23]**MD5: 9f059c973637f105271d345a95787a5f** -
detected by 2 out of 45 antivirus scanners as
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[24]**MD5: f179a067580014b1e16900b90d90a872** -
detected by 2 out of 47 antivirus scanners as
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[25]**MD5: aef4f659943cbc530e4e1b601e75b19e** -
detected by 2 out of 46 antivirus scanners as
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[26]**MD5: 8a00786ed6939a8ece2765d503c97ff8** -
detected by 2 out of 45 antivirus scanners as
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[27]**MD5: 868fcf05827c092fa1939930c2f50016** -
detected by 2 out of 45 antivirus scanners as
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[28]**MD5: a6ef49789845ed1a66f94fd7cc089e1b** -
detected by 2 out of 47 antivirus scanners as
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[29]**MD5: 22aa473772b2dfb0f019dac3b8749bb6** -
detected by 2 out of 45 antivirus scanners as
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[30]**MD5: 52b74046d0c123772566d591524b3bf7** -
detected by 2 out of 46 antivirus scanners as
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[31]**MD5: bbff61a2e3555a6675bc77621be19a73** -
detected by 2 out of 46 antivirus scanners as

Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[32]**Cybercrime-friendly affiliate networks** continue, and will continue to represent a major driving factor be-

hind the growth of any market segment within the cybercrime system, as they result in a win-win-lose scenario for

their operations, participants and the potential victims of the fraudulent/malicious propositions/releases courtesy of these networks.

With mobile traffic acquisition available on demand based on any given preference a potential could have, cy-

bercriminals would continue converting it into victims, cashing in on their overall lack of awareness of the TTPs of today's modern cybercriminals.

Updates will be posted as soon as new developments take place.

1. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>
2. <http://www.webroot.com/blog/tag/affiliate-networks/>
3. <http://www.webroot.com/blog/2013/09/18/affiliate-network-mobile-malware-impersonates-google-play-tricks-users-installing-premium-rate-sms-sending-rogue-apps/>

4. http://ddanchev.blogspot.com/2007/05/commercializing-mobile-malware_18.html

5. <http://ddanchev.blogspot.com/2008/07/mobile-malware-scam-isexplorer-wants.html>

6. <http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html>

7. <http://www.internetnews.com/wireless/article.php/3584431>

8. <http://ddanchev.blogspot.com/2009/07/transmitterc-mobile-malware-in-wild.html>

9. <http://www.webroot.com/blog/2013/10/25/cybercriminals-release-new-commercially-available-androidblackberry-supporting-mobile-malware-bot/>

10. <http://ddanchev.blogspot.com/2013/07/a-peek-inside-managed-otpatstan-token.html>

11. <http://www.webroot.com/blog/2013/09/18/affiliate-network-mobile-malware-impersonates-google-play-tricks-users-installing-premium-rate-sms-sending-rogue-apps/>

12. <http://www.webroot.com/blog/2013/08/13/cybercrime-friendly-underground-traffic-exchange-helps-facilitate->

[778](#)

[fraudulent-and-malicious-activity/](#)

13. <http://www.webroot.com/blog/2013/08/29/cybercrime-friendly-underground-traffic-exchanges-help-facilitate-fraudulent-and-malicious-activity-part-two/>

14. <https://www.virustotal.com/en/file/1a3e255ccb734021ff8c89b4f14196d065fa1905ab5df398431df4909b1ed1d7/analysis/>

15. <https://www.virustotal.com/en/file/5a0f6fe6d46d6bda81a237d72a60ec55df7062be4dff1abe7712d64d1a6a9a1f/analysis/1383771675/>

16. <https://www.virustotal.com/en/file/61dd75041770fb177a76658bf620b8568aec47d3c8c779d94913e549090479f8/analysis/1383771784/>

17. <https://www.virustotal.com/en/file/195a3be1048d9b8192670a488cf991b39d6ff6c8a3d2996dfef30633fe9eeac5/analysis/1383771850/>

18. <https://www.virustotal.com/en/file/5c19a007d6620c542940a2ebf441db7a4285ee42cea2e4e4b153aab80b44fa4d/analysis/1383771922/>

19.

<https://www.virustotal.com/en/file/669e7c760993098bfe6f1deb595239ace7809a9674ef5eef0e48631d6743bf04/analysis/1383772019/>

[is/1383772019/](https://www.virustotal.com/en/file/669e7c760993098bfe6f1deb595239ace7809a9674ef5eef0e48631d6743bf04/analysis/1383772019/)

20.

<https://www.virustotal.com/en/file/0826d6b1d5c803afaec09299e7df3f2763cb39dba91854346fc57d7f610d9299/analysis/1383772147/>

[is/1383772147/](https://www.virustotal.com/en/file/0826d6b1d5c803afaec09299e7df3f2763cb39dba91854346fc57d7f610d9299/analysis/1383772147/)

21.

<https://www.virustotal.com/en/file/941bee13931948d2913982efb0d677a2222648ef23893e7cbf773c59bb5ea369/analysis/1383772232/>

[s](https://www.virustotal.com/en/file/941bee13931948d2913982efb0d677a2222648ef23893e7cbf773c59bb5ea369/analysis/1383772232/)

[is/1383772232/](https://www.virustotal.com/en/file/941bee13931948d2913982efb0d677a2222648ef23893e7cbf773c59bb5ea369/analysis/1383772232/)

22.

<https://www.virustotal.com/en/file/6cf9503053e927c75a537b2574fa44e203f5fc4079a6446e8b285b13ad8bbf7f/analysis/1383772324/>

[is/1383772324/](https://www.virustotal.com/en/file/6cf9503053e927c75a537b2574fa44e203f5fc4079a6446e8b285b13ad8bbf7f/analysis/1383772324/)

23.

<https://www.virustotal.com/en/file/03734e0e1dc2a834e4892f10cfa52399180cac37579bfd742ea81fa5503e18ff/analysis/1383772403/>

[is/1383772403/](https://www.virustotal.com/en/file/03734e0e1dc2a834e4892f10cfa52399180cac37579bfd742ea81fa5503e18ff/analysis/1383772403/)

24.

<https://www.virustotal.com/en/file/f7a8d5bf295dcc0d614ccb10a25aaa7645c9f6c5240da481bf18bbe9f050e8cd/analysis/1383783939/>

[is/1383783939/](https://www.virustotal.com/en/file/f7a8d5bf295dcc0d614ccb10a25aaa7645c9f6c5240da481bf18bbe9f050e8cd/analysis/1383783939/)

25.

<https://www.virustotal.com/en/file/77779337b988c5c4a606cb5299c0cb92e39766ae05d3cbe5dc005064d1059eb4/analysis/>

[is/1383784127/](#)

26.

<https://www.virustotal.com/en/file/5e9963185d18b01a5900d53f436c70ea4260de9327e52ef97107a755ca60b570/analysis/>

[is/1383784229/](#)

27.

<https://www.virustotal.com/en/file/c618d84e47ef2ccdd11d7a2f3883e5fa7bca52442bf3a0904e1723f3dc459461/analysis/>

[is/1383784294/](#)

28.

<https://www.virustotal.com/en/file/62f4c45a5f698c759e66187d6d322b476e78d973aa6bf6daabcebb2d6139ad2d/analysis/>

[is/1383784390/](#)

29.

<https://www.virustotal.com/en/file/26c88732e4895244a937553c25bce2378718fc4e5af0977abdb6cedc9dbb9fbb/analysis/>

[is/1383784546/](#)

30.

<https://www.virustotal.com/en/file/0713ef64ca57ab7164142f485208dba9cace1b8f9da3fdaaa0c840541df6b843/analysis/>

[is/1383784624/](#)

31.

<https://www.virustotal.com/en/file/f8b10b6ae34c01878d24fd3bf29235b117303dd17b720e15126f0cc6a3110adf/analysis/1383785064/>

[is/1383785064/](#)

32. <http://www.zdnet.com/blog/security/inside-an-affiliate-spam-program-for-pharmaceuticals/2054>

779



New Commercially Available Modular Malware Platform Released On the Underground Marketplace

(2013-11-13 00:15)

Cybercriminals have recently released a new (v3 to be more precise indicating possible beneath the radar operation

until now), commercially available, modular malware platform, including such cybercrime-friendly features like

DNS Changer, Loaders, [1]**Injects**, and [2]**Ransomware** features – completely blocking the Internet access of [3]**the affected user** in this particular case – with several upcoming modules such as stealth VNC, and Remote IE (a feature which would allow them to completely hijack any sort of encrypted session taking place on the affected host,

naturally including the cookies).

Sample screenshots of the command and control interface+DNS Changer in action:



With prices for the standard package starting from \$1,500, I expect that the malware bot will quickly gain market

share thanks to its compatibility with existing/working crimeware concepts/releases, as well as thanks to the general

availability of 24/7/365 [4]**managed malware crypting services**, applying the necessary degree of QA (Quality

Assurance) to a potential campaign before launching it. Moreover, yet another factor that would greatly contribute

to the success of such type of newly released platforms is the the ease of acquisition of legitimate traffic – think

[5]**blackhat SEO**, [6]**compromised FTP accounts**, or [7]**mass SQL injection campaigns** – to be later on converted into malware-infected hosts, most commonly through social engineering, or the client-side exploitation of outdated and

already patched vulnerabilities in browser plugins/third-party applications.

Furthermore, with or without the full scale modularity in place – some of the modules are currently in the

works, as well as the lack of built-in renting/reselling/traffic acquisition/affiliate network type of monetization

elements, typical for what can be best described as platform type of underground market release compared to a

standalone modular malware bot, the bot's worth keeping an eye on.

The DNS Changer IP seen in the screenshot **62.76.176.214** (*62-76-176-214.clodo.ru*), can also be connected to

related malicious activity. For instance, [8]**MD5: cef012fb4fa7cd55f04558ecee04cd4e** is known to have previously

phoned back to **62.76.176.214**.

And most interestingly, [9]**according to this assessment**, next to phoning back to 62.76.176.214, the following

malicious domains are also known to have been used as C &Cs by the same sample:

6r3u8874dfd9.com - known to have responded to 31.170.179.179

r55u87799hd39.com - known to have responded to 31.170.179.179

r95u8114dfd9.com

The following malicious MD5s are also known to have phoned back to the same C &C IP (31.170.179.179)

since the beginning of the month:

MD5: 56f05611ec91f010d015536b7e9fe1a5

781

MD5: 49aeaa9fad5649d20a9c56e611e81d96

MD5: bf4fa138741ec4af0a0734b28142f7ae

MD5: cd92df2172a40ebb507fa701dcb14fea

MD5: 1d51cde1ab7a1d3d725e507089d3ba5e

MD5: a00695df0a50b3d3ffeb3454534d97a8

MD5: ea8340c95589ca522dac1e04839a9ab9

MD5: f2933ca59e8453a2b50f6d38a9ad9709

MD5: dd9c4ba82de8dcf0f3e440b302e223e8

MD5: d92ad37168605579319c3dff4d6e8c26

MD5: 004bf3f6b7f49d5c650642dde3255b16

MD5: deb8bcd6c7987ee4e0a95273e76feccd

MD5: 1791cb3e3da28aec11416978f415dcd3

MD5: 7eae6322c9dcaa0f12a99f2c52b70224

MD5: 0027511d25a820bcd7565257fd61ba4

MD5: 294edcdaab9ce21cb453dc40642f1561

MD5: b414d9f54a723e8599593503fe0de4f1

MD5: 20ee0617e7dc03c571ce7d5c2ee6a0a0

MD5: e1059ae3fb9c62cf3272eb6449de23cf

This post has been reproduced from [10]Dancho Danchev's blog . Follow him [11]on Twitter.

1. <http://ddanchev.blogspot.com/2013/07/a-peek-inside-managed-otpatstan-token.html>

2. <http://www.webroot.com/blog/tag/ransomware/>
3. <https://www.google.com/webhp?tab=ww&ei=#q=site:ddanchev.blogspot.com+ransomware>
4. <https://www.google.com/webhp?tab=ww&ei=#q=site:webroot.com%2Fblog+crypting>
5. <https://www.google.com/webhp?tab=ww&ei=#q=site:ddanchev.blogspot.com+blackhat+seo>
6. <https://www.google.com/webhp?tab=ww&ei=#q=site:ddanchev.blogspot.com+ftp+accounts>
7. <https://www.google.com/webhp?tab=ww&ei=#q=site:ddanchev.blogspot.com+sql+injection>
8. <https://www.virustotal.com/en/file/4ca375c6db3d32dde7b981b0981079d8e13bd121a81c835d58d02a046d98277f/analysis/>
9. http://www.symantec.com/security_response/writeup.jsp?docid=2013-101610-5035-99&tabid=2
10. <http://ddanchev.blogspot.com/>
11. <http://twitter.com/danchodanchev>

782



New Commercially Available Modular Malware Platform Released On the Underground Marketplace

(2013-11-13 00:15)

Cybercriminals have recently released a new (v3 to be more precise indicating possible beneath the radar operation

until now), commercially available, modular malware platform, including such cybercrime-friendly features like

DNS Changer, Loaders, [1]**Injects**, and [2]**Ransomware** features – completely blocking the Internet access of [3]**the affected user** in this particular case – with several upcoming modules such as stealth VNC, and Remote IE (a feature which would allow them to completely hijack any sort of encrypted session taking place on the affected host, naturally including the cookies).

Sample screenshots of the command and control interface+DNS Changer in action:

783



With prices for the standard package starting from \$1,500, I expect that the malware bot will quickly gain market

share thanks to its compatibility with existing/working crimeware concepts/releases, as well as thanks to the general

availability of 24/7/365 [4]**managed malware crypting services**, applying the necessary degree of QA (Quality

Assurance) to a potential campaign before launching it. Moreover, yet another factor that would greatly contribute

to the success of such type of newly released platforms is the the ease of acquisition of legitimate traffic – think

[5]**blackhat SEO**, [6]**compromised FTP accounts**, or [7]**mass SQL injection campaigns** – to be later on converted into malware-infected hosts, most commonly through social engineering, or the client-side exploitation of outdated and

already patched vulnerabilities in browser plugins/third-party applications.

Furthermore, with or without the full scale modularity in place – some of the modules are currently in the

works, as well as the lack of built-in renting/reselling/traffic acquisition/affiliate network type of monetization

elements, typical for what can be best described as platform type of underground market release compared to a

standalone modular malware bot, the bot's worth keeping an eye on.

The DNS Changer IP seen in the screenshot **62.76.176.214** (*62-76-176-214.clodo.ru*), can also be connected to

related malicious activity. For instance, [8]**MD5: cef012fb4fa7cd55f04558ecee04cd4e** is known to have previously

phoned back to **62.76.176.214**.

And most interestingly, [9]**according to this assessment**, next to phoning back to 62.76.176.214, the following

malicious domains are also known to have been used as C &Cs by the same sample:

6r3u8874dfd9.com - known to have responded to 31.170.179.179

r55u87799hd39.com - known to have responded to 31.170.179.179

r95u8114dfd9.com

The following malicious MD5s are also known to have phoned back to the same C &C IP (31.170.179.179)

since the beginning of the month:

MD5: 56f05611ec91f010d015536b7e9fe1a5

784

MD5: 49aeaa9fad5649d20a9c56e611e81d96

MD5: bf4fa138741ec4af0a0734b28142f7ae

MD5: cd92df2172a40ebb507fa701dcb14fea

MD5: 1d51cde1ab7a1d3d725e507089d3ba5e

MD5: a00695df0a50b3d3ffeb3454534d97a8

MD5: ea8340c95589ca522dac1e04839a9ab9

MD5: f2933ca59e8453a2b50f6d38a9ad9709

MD5: dd9c4ba82de8dcf0f3e440b302e223e8

MD5: d92ad37168605579319c3dff4d6e8c26

MD5: 004bf3f6b7f49d5c650642dde3255b16

MD5: deb8bcd6c7987ee4e0a95273e76feccd

MD5: 1791cb3e3da28aec11416978f415dcd3

MD5: 7eae6322c9dcaa0f12a99f2c52b70224

MD5: 0027511d25a820bcd7565257fd61ba4

MD5: 294edcdaab9ce21cb453dc40642f1561

MD5: b414d9f54a723e8599593503fe0de4f1

MD5: 20ee0617e7dc03c571ce7d5c2ee6a0a0

MD5: e1059ae3fb9c62cf3272eb6449de23cf

Updates will be posted as soon as new developments take place.

1. <http://ddanchev.blogspot.com/2013/07/a-peek-inside-managed-otpatstan-token.html>
2. <http://www.webroot.com/blog/tag/ransomware/>
3. <https://www.google.com/webhp?tab=ww&ei=#q=site:ddanchev.blogspot.com+ransomware>
4. <https://www.google.com/webhp?tab=ww&ei=#q=site:webroot.com%2Fblog+crypting>
5. <https://www.google.com/webhp?tab=ww&ei=#q=site:ddanchev.blogspot.com+blackhat+se>

o

6. <https://www.google.com/webhp?tab=ww&ei=#q=site:ddanchev.blogspot.com+ftp+accounts>

7. <https://www.google.com/webhp?tab=ww&ei=#q=site:ddanchev.blogspot.com+sql+injection>

8. <https://www.virustotal.com/en/file/4ca375c6db3d32dde7b981b0981079d8e13bd121a81c835d58d02a046d98277f/analysis/>

[is/](#)

9. http://www.symantec.com/security_response/writeup.jsp?docid=2013-101610-5035-99&tabid=2

785



Fake Chrome/Firefox/Internet Explorer/Safari Updates Expose Users to Android Malware (2013-11-14 16:38)

A currently ongoing [1]**malicious campaign using compromised sites as the primary traffic acquisition tactic**, is

attempting to socially engineer users (English and Russian speaking) into thinking that they're using an outdated

version of their browser, and need to apply a bogus (security/antivirus) update. In reality though, the update is a

variant of Trojan:Android/Fakeinst.EQ/Android.SmsSend.

Sample screenshots of the fake browser update landing pages:

786



787



**Social
engineering
redirection
chain:**

hxxp://france-leasebacks.com/includes/domit/1.php

->

*hxxp://advertcliks.net/ir/28/1405/56e9ca1335c2773445a79
d5ddf75a755/tl*

(93.115.82.239;

Email:

maxax-

*aha@gmail.com) -> hxxp://newupdateronline.org
(109.163.230.182; Email: vbistrih@yandex.com).*

Known to have responded to 109.163.230.182 are also the following domains:

1mc8.asia

anglecultivatep.in

appallinglyndiscoveries.in

bilious-6biros.in

788

boathire.pw

cvwv87.pro

dlscncncnew1.pw

efuv77.pro

familye-perspex.in

farting-meagre.in

flvupdate.in

fringeclamberedk.in

hopefully-great8.in

investment-growsa.asia

money-tree.pw

moon-media.pw

moontree.pw

mountainlake.pw

movingv-relation.in

new-updateronline.org

Sample Android samples pushed by the campaign:

[2]MD5:

da7fffa08bdeb945ca8237c2894aedd0 - detected by 11 out of 46 antivirus scanners as An-

droid.SmsSend.809.origin; Android.Trojan.FakeInst.HE

[3]MD5: 1e1f57f6c8c9fb39da8965275548174f -

detected by 17 out of 46 antivirus scanners as HEUR:Trojan-

SMS.AndroidOS.FakeInst.fe; Andr/RuSms-AL

[4]MD5: b0f597636859b7f5b2c1574d7a8bbbbbb -

detected by 13 out of 47 antivirus scanners as HEUR:Trojan-

SMS.AndroidOS.FakeInst.fe; Andr/RuSms-AL

[5]MD5: b40aebc327e1bc6aabe5ccb4f18e8ea4 -

detected by 16 out of 48 antivirus scanners as
Android:FakeIns-AF;

Trojan:Android/Fakeinst.EQ

All samples phone back to **dlcdcncnew.net**

(109.163.230.182; Email: constantin.zawyalov@yandex.ru).

Re-

sponding to the same IP is also **newapk-flv.org**.

The same email is also known to have been previously used to register the following domains:

downloader8days.in

open-filedownload4.in (known to have responded to 188.95.159.30)

upweight.in

bestnewbrowsers.in

bestowedcomedyb.org (known to have responded to 109.163.230.180)

expandload.in

2012internet-load.in

4interfilefolder.in

99030.in

admitted-6crept.org

rufilesserver.in

It appears that the traffic is not segmented – to [6]**affect mobile device users only** – at any point of the redi-

rection chain, an indication of what I believe is a boutique cybercrime-friendly operation. In comparison, the

relatively more sophisticated ones would segment the traffic, usually acquired through the [7]**active exploitation of**

tens of thousands of legitimate Web sites, or the direct purchase of segmented mobile traffic.

Interestingly, both novice players in this market segment, and the experienced ones, are implementing basic

evasive tactics, such as, for instance, the need to provide a valid mobile number, where a potential victim will receive

789

a confirmation code for accessing the inventory of rogue games and applications, thereby preventing automatic acquisition of the apps for further analysis. Moreover, providing a valid mobile number to the cybercriminals behind

the campaign, is naturally prone to be abused in ways largely based on the preferences of those who obtained them

through such a way, therefore users are advised not to treat their mobile number in a privacy conscious way.

This post has been reproduced from [8]Dancho Danchev's blog . Follow him [9]on Twitter.

1. <http://ddanchev.blogspot.com/2013/09/rogue-iframe-injected-web-sites-lead-to.html>

2. <https://www.virustotal.com/en/file/2ef49d2ba03c8d9420e008edb8d04fb3abad2fd41684e65d0d47ef5fc4d2787a/analysis/>

3.

<https://www.virustotal.com/en/file/65bb64a9e651ea785d2ba92c2ab8bd02f6353ae472bf2bc5f917b79bfdf67a10/analysis/>

[is/](#)

4.

<https://www.virustotal.com/en/file/7e7528e5a1f2328c8e5167ad51c4cda8791f5b213cd85a436bdd83681b8ad7f6/analysis/>

[s](#)

[is/](#)

5.

<https://www.virustotal.com/en/file/52dfd24ce2af44c37f5cb8cd7ed37bc0c62bff5148293b891cc5ef558fdc5369/analysis/>

[is/](#)

6. <http://www.webroot.com/blog/2013/01/22/android-malware-spreads-through-compromised-legitimate-web-sites/>

7. <http://ddanchev.blogspot.com/2013/09/rogue-iframe-injected-web-sites-lead-to.html>

8. <http://ddanchev.blogspot.com/>

9. <http://twitter.com/danchodanchev>

790



Fake Chrome/Firefox/Internet Explorer/Safari Updates Expose Users to Android Malware (2013-11-14 16:38)

A currently ongoing [1]**malicious campaign using compromised sites as the primary traffic acquisition tactic**, is

attempting to socially engineer users (English and Russian speaking) into thinking that they're using an outdated

version of their browser, and need to apply a bogus (security/antivirus) update. In reality though, the update is a

variant of Trojan:Android/Fakeinst.EQ/Android.SmsSend.

Sample screenshots of the fake browser update landing pages:

791



792



**Social
engineering
redirection
chain:**

hxxp://france-leasebacks.com/includes/domit/1.php

->

hxxp://advertcliiks.net/ir/28/1405/56e9ca1335c2773445a79d5ddf75a755/tl

(93.115.82.239;

Email:

maxax-

*aha@gmail.com) -> hxxp://newupdateronline.org
(109.163.230.182; Email: vbistrih@yandex.com).*

Known to have responded to 109.163.230.182 are also the following domains:

1mc8.asia

anglecultivatep.in

appallinglyndiscoveries.in

bilious-6biros.in

793

boathire.pw

cvwv87.pro

dlldcncnew1.pw

efuv77.pro

familye-perspex.in

farting-meagre.in

flvupdate.in

fringeclamberedk.in

hopefully-great8.in

investment-growsa.asia

money-tree.pw

moon-media.pw

moontree.pw

mountainlake.pw

movingv-relation.in

new-updateronline.org

Sample Android samples pushed by the campaign:

[2]MD5:

da7fffa08bdeb945ca8237c2894aedd0 - detected by 11 out of 46 antivirus scanners as An-

droid.SmsSend.809.origin; Android.Trojan.FakeInst.HE

[3]MD5: 1e1f57f6c8c9fb39da8965275548174f - detected by 17 out of 46 antivirus scanners as HEUR:Trojan-

SMS.AndroidOS.FakeInst.fe; Andr/RuSms-AL

[4]MD5: b0f597636859b7f5b2c1574d7a8bbbbbb - detected by 13 out of 47 antivirus scanners as HEUR:Trojan-

SMS.AndroidOS.FakeInst.fe; Andr/RuSms-AL

[5]**MD5: b40aebc327e1bc6aabe5ccb4f18e8ea4** -
detected by 16 out of 48 antivirus scanners as
Android:FakeIns-AF;

Trojan:Android/Fakeinst.EQ

All samples phone back to **dlldcncnew.net**
(109.163.230.182; Email: constantin.zawyalov@yandex.ru).

Re-

sponding to the same IP is also **newapk-flv.org**.

**The same email is also known to have been
previously used to register the following domains:**

downloader8days.in

open-filedownload4.in (known to have responded to
188.95.159.30)

upweight.in

bestnewbrowsers.in

bestowedcomedyb.org (known to have responded to
109.163.230.180)

expandload.in

2012internet-load.in

4interfilefolder.in

99030.in

admitted-6crept.org

rufileserver.in

It appears that the traffic is not segmented – to [6]**affect mobile device users only** – at any point of the redi-

rection chain, an indication of what I believe is a boutique cybercrime-friendly operation. In comparison, the

relatively more sophisticated ones would segment the traffic, usually acquired through the [7]**active exploitation of**

tens of thousands of legitimate Web sites, or the direct purchase of segmented mobile traffic.

Interestingly, both novice players in this market segment, and the experienced ones, are implementing basic

evasive tactics, such as, for instance, the need to provide a valid mobile number, where a potential victim will receive

794

a confirmation code for accessing the inventory of rogue games and applications, thereby preventing automatic acquisition of the apps for further analysis.

Moreover, providing a valid mobile number to the cybercriminals behind the campaign, is naturally prone to

be abused in ways largely based on the preferences of those who obtained them through such a way, therefore users

are advised not to treat their mobile number in a privacy conscious way.

Updates will be posted as soon as new developments take place.

1. <http://ddanchev.blogspot.com/2013/09/rogue-iframe-injected-web-sites-lead-to.html>
2. <https://www.virustotal.com/en/file/2ef49d2ba03c8d9420e008edb8d04fb3abad2fd41684e65d0d47ef5fc4d2787a/analysis/>
3. <https://www.virustotal.com/en/file/65bb64a9e651ea785d2ba92c2ab8bd02f6353ae472bf2bc5f917b79bdfd67a10/analysis/>
4. <https://www.virustotal.com/en/file/7e7528e5a1f2328c8e5167ad51c4cda8791f5b213cd85a436bdd83681b8ad7f6/analysis/>
5. <https://www.virustotal.com/en/file/52dfd24ce2af44c37f5cb8cd7ed37bc0c62bff5148293b891cc5ef558fdc5369/analysis/>
6. <http://www.webroot.com/blog/2013/01/22/android-malware-spreads-through-compromised-legitimate-websites/>
7. <http://ddanchev.blogspot.com/2013/09/rogue-iframe-injected-web-sites-lead-to.html>

795

1.12

December

796



Summarizing Webroot's Threat Blog Posts for November (2013-12-03 23:38)

The following is a brief summary of all of my posts at [1]**Webroot's Threat Blog** for November, 2013. You can

subscribe to [2]**Webroot's Threat Blog RSS Feed**, or follow me on Twitter:

01. [3]Google-dorks based mass Web site hacking/SQL injecting tool helps facilitate malicious online activity

02. [4]Deceptive ads lead to the SpyAlertApp PUA (Potentially Unwanted Application)

03.

[5]Cybercriminals differentiate their 'access to compromised PCs' service proposition, emphasize on the

prevalence of 'female bot slaves'

04. [6]New vendor of 'professional DDoS for hire service' spotted in the wild

05. [7]Source code for proprietary spam bot offered for sale, acts as force multiplier for cybercrime-friendly activity **06.**

[8]Low Quality Assurance (QA) iframe campaign linked to May's Indian government Web site compromise spotted

in the wild

07. [9]Popular French torrent portal tricks users into installing the BubbleDock/Downware/DownloadWare PUA

(Potentially Unwanted Application)

797

08. [10]Web site of Brazilian 'Prefeitura Municipal de Jaqueira' compromised, leads to fake Adobe Flash player **09.**

[11]Malicious multi-hop iframe campaign affects thousands of Web sites, leads to a cocktail of client-side exploits **10.**

[12]Vendor of TDoS products/services releases new multi-threaded SIP-based TDoS tool

11. [13]Cybercriminals spamvertise tens of thousands of fake 'Sent from my iPhone' themed emails, expose users to

malware

12. [14]Fake 'Annual Form (STD-261) - Authorization to Use Privately Owned Vehicle on State Business' themed

emails lead to malware

13. [15]'Newly released proxy-supporting Origin brute-forcing tools targets users with weak passwords'

14. [16]Fake WhatsApp 'Voice Message Notification' themed emails expose users to malware

15. [17]Cybercriminals impersonate HSBC through fake 'payment e-Advice' themed emails, expose users to malware

16. [18]Fake 'MMS Gallery' notifications impersonate T-Mobile U.K, expose users to malware

17. [19]Fake 'October's Billing Address Code' (BAC) form themed spam campaign leads to malware

This post has been reproduced from [20]Dancho Danchev's blog . Follow him [21]on Twitter.

1. <http://www.webroot.com/blog>
2. <http://feeds2.feedburner.com/WebrootThreatBlog>
3. <http://www.webroot.com/blog/2013/11/01/peek-inside-google-dorks-based-mass-sql-injecting-tool/>
4. <http://www.webroot.com/blog/2013/11/01/deceptive-ads-lead-spyalertapp-pua-potentially-unwanted-application/>
5. <http://www.webroot.com/blog/2013/11/04/cybercriminals-differentiate-access-compromised-pcs-service-proposition-emphasize-prevalence-female-bot-slaves/>
6. <http://www.webroot.com/blog/2013/11/05/new-vendor-professional-ddos-hire-service-spotted-wild/>
7. <http://www.webroot.com/blog/2013/11/07/source-code-proprietary-spam-bot-offered-sale-acts-force-multiplier-cybercrime-friendly-activity/>
8. <http://www.webroot.com/blog/2013/11/08/low-quality-assurance-ga-iframe-campaign-linked-mays-india-government-web-site-compromise-spotted-wild/>
9. <http://www.webroot.com/blog/2013/11/11/popular-french-torrent-portal-tricks-users-into/>
10. <http://www.webroot.com/blog/2013/11/12/web-site-brazilian-prefeitura-municipal-de-jaqueira-compromised-le>

[ads-fake-adobe-flash-player/](#)

11. <http://www.webroot.com/blog/2013/11/13/malicious-multi-hop-iframe-campaign-affects-thousands-of-web-sites-leads-to-cve-2011-3402/>

12. <http://www.webroot.com/blog/2013/11/15/vendor-tdos-productsservices-releases-new-multi-threaded-sip-based-tdos-tool/>

13. <http://www.webroot.com/blog/2013/11/19/cybercriminals-spamvertise-tens-thousands-fake-sent-iphone-themed-emails-expose-users-malware/>

14. <http://www.webroot.com/blog/2013/11/20/fake-annual-form-std-261-authorization-use-privately-owned-vehicle-state-business-themed-emails-lead-malware/>

15. <http://www.webroot.com/blog/2013/11/21/newly-released-proxy-supporting-origin-brute-forcing-tools-targets-users-weak-passwords/>

16. <http://www.webroot.com/blog/2013/11/22/fake-whatsapp-voice-message-notification-themed-emails-expose-user-s-malware/>

17. <http://www.webroot.com/blog/2013/11/25/cybercriminals-impersonate-hsbc-fake-payment-e-advice-themed-email>

[s-expose-users-malware/](#)

18. <http://www.webroot.com/blog/2013/11/26/fake-mms-gallery-notifications-impersonate-t-mobile-u-k-expose-users-malware/>

19. <http://www.webroot.com/blog/2013/11/27/fake-octobers-billing-address-code-bac-form-themed-spam-campaign-leads-malware/>

20. <http://ddanchev.blogspot.com/>

21. <http://twitter.com/danchodanchev>

798



Facebook Circulating 'Who's Viewed Your Profile' Campaign Exposes 800k+ Users to CrossRider

PUA/Rogue Firefox Add-ons/Android Adware AirPush (2013-12-04 02:25)

A massive privacy-violating, Facebook circulating "Who's Viewed Your Profile" campaign, has been operating beneath the radar, exposing over 800,000 users internationally, to a cocktail of [1]**PUAs (Potentially Unwanted Applications)**, rogue Firefox Add-ons impersonating Adobe's Flash Player, as well as the Android based adware AirPush.

Relying on a proven social engineering tactic of "offering what's not being offered in general", next to hosting the rogue files on legitimate service providers – Google Docs and Dropbox in this particular case – the campaign is a

great example that the ubiquitous for the social network social engineering scheme, continues to trick gullible and

uninformed users into installing privacy-violating applications on their hosts/mobile devices.

Let's dissect the campaign, expose its infrastructure, (conservatively) assess the damage, and provide fresh

MD5s for the currently served privacy-violating PUAs, Firefox add-ons, and Android adware.

Primary spamvertised Facebook URL: *FCOSYUC.tk/?15796422*

Redirection

chain:

p2r0f3rviewer9890.co.nf

->

bit.ly/1bZCeNv?vsdvc

->

wh0prof.uni.me/?sdvsjka

->

wh0prof.uni.me/ch/

Rogue

Google

Store

Extension

URL

(currently

offline):

hxxps://chrome.google.com/webstore/detai-

l/dllaajfgpigkeblmlbamflggfjk gbej

Campaign's GA Account ID: *UA-12798017-1*

799



Domain name reconnaissance:

wh0prof.uni.me - 192.157.201.42

Known to have responded to the same IP are also the following domains:

cracks4free.info

pr0lotra.p9.org

Google Docs Hosted PUA URLs:

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCcuQwqVFljUDBnTjFHdVE &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCcuQwqRXBMLWZ4cVZJV2s &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCcuQwqUjlLLWc4MVFRQUk &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqOXlyNko0VFBOdnM &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqZm5yeUFudFhqclU &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqbWpfNW5FalJmRGM &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqS3V1ZkZBQjJGbjQ &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqX2xXbEJLbEY0Q3M &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqMU5RVkJSWURxME0 &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqVFijUDBnTjFHdVE &export=download

Dropbox Firefox Add-on/Android APK Hosted URLs:

*hxxps://dl.dropboxusercontent.com/s/so3vm50w298qkto/W
hoViewsYourProfile.apk*

*hxxps://dl.dropboxusercontent.com/s/kor9c2mqv49esva/kka
dobe-ff.xpi*

800



**Detection rate for the served PUAs, the Android
adware and the rogue Firefox Add-on:**

[2]MD5:

c7fcf7078597ea752b8d54e406c266a7 - detected by 5 out of 48 antivirus scanners as

PUP.Optional.CrossRider

[3]**MD5: 30cf98d7dc97cae57f8d72487966d20b** - detected by 6 out of 48 antivirus scanners as Trojan.Dropper.FB

[4]**MD5:**

f2459b6bde1d662399a3df725bf8891b - detected by 13 out of 48 antivirus scanners as Ad-

ware/AirPush!Android; Android Airpush; Adware/ANDR.Airpush.G.Gen

[5]**MD5:**

3fb95e1ed77d1b545cf7385b4521b9ae - detected by 18 out of 48 antivirus scanners as

JS/TrojanClicker.Agent.NDL

Once executed **MD5: 30cf98d7dc97cae57f8d72487966d20b** phones back to 195.167.11.4.

Time to (conservatively) assess the campaign's damage over the year(s):

801



802



The click-through rate should be considered conservative, and it remains unknown whether the URL shortening

service was used by the cybercriminal(s) since day one of the campaign.

803



The campaign remains active, and is just the tip of the iceberg in terms of similar campaigns tricking Facebook's

users into thinking that they can eventually see who's viewed their profile. Facebook users who stumble across such

campaigns on their own, or their friends' Walls, are advised [6]**to consider reporting the campaign back to Facebook**, immediately.

This post has been reproduced from [7]Dancho Danchev's blog . Follow him [8]on Twitter.

1. <http://www.webroot.com/blog/tag/pua/>

2. <https://www.virustotal.com/en/file/ecd6bb6e53477496ea45de362012b4b1d458ee966867eb89ea4005c5bd9fe8b3/analysis/1385988722/>

[is/1385988722/](https://www.virustotal.com/en/file/ecd6bb6e53477496ea45de362012b4b1d458ee966867eb89ea4005c5bd9fe8b3/analysis/1385988722/)

3.

<https://www.virustotal.com/en/file/b44aabb0e235d36377f3cd55ec4af596a89c0a7814103369d3f48d54d29ffcc7/analysis/1385988808/>

[is/1385988808/](https://www.virustotal.com/en/file/b44aabb0e235d36377f3cd55ec4af596a89c0a7814103369d3f48d54d29ffcc7/analysis/1385988808/)

4.

<https://www.virustotal.com/en/file/72f3834e9c8ee164b7e82383415da822579ffb23fbfa7f55ac650a22b2386ee0/analysis/1386108420/>

[is/1386108420/](https://www.virustotal.com/en/file/72f3834e9c8ee164b7e82383415da822579ffb23fbfa7f55ac650a22b2386ee0/analysis/1386108420/)

804

5.

<https://www.virustotal.com/en/file/3b25b67592b9b06fca05ab61abd16559e7c94f9ac3c225e5ae00ddc5318923c6/analysis/1386109278/>

[ys](https://www.virustotal.com/en/file/3b25b67592b9b06fca05ab61abd16559e7c94f9ac3c225e5ae00ddc5318923c6/analysis/1386109278/)

[is/1386109278/](https://www.virustotal.com/en/file/3b25b67592b9b06fca05ab61abd16559e7c94f9ac3c225e5ae00ddc5318923c6/analysis/1386109278/)

6. <https://www.facebook.com/help/www/117257561692875>

7. <http://ddanchev.blogspot.com/>

8. <http://twitter.com/danchodanchev>

805



Facebook Circulating 'Who's Viewed Your Profile' Campaign Exposes 800k+ Users to CrossRider

PUA/Rogue Firefox Add-ons/Android Adware AirPush (2013-12-04 02:25)

A massive privacy-violating, Facebook circulating "Who's Viewed Your Profile" campaign, has been operating beneath the radar, exposing over 800,000 users internationally, to a cocktail of [1]**PUAs (Potentially Unwanted Applications)**, rogue Firefox Add-ons impersonating Adobe's Flash Player, as well as the Android based adware AirPush.

Relying on a proven social engineering tactic of "offering what's not being offered in general", next to hosting the rogue files on legitimate service providers - Google Docs and Dropbox in this particular case - the campaign is a

great example that the ubiquitous for the social network social engineering scheme, continues to trick gullible and

uninformed users into installing privacy-violating applications on their hosts/mobile devices.

Let's dissect the campaign, expose its infrastructure, (conservatively) assess the damage, and provide fresh

MD5s for the currently served privacy-violating PUAs, Firefox add-ons, and Android adware.

Primary spamvertised Facebook URL: *FCOSYUC.tk/?15796422*

Redirection

chain:

p2r0f3rviewer9890.co.nf

->

bit.ly/1bZCeNv?vsdvc

->

wh0prof.uni.me/?sdvsjka

->

wh0prof.uni.me/ch/

Rogue

Google

Store

Extension

URL

(currently

offline):

hxxps://chrome.google.com/webstore/detai-

l/dllaajfgpigkeblmlbamflggfjk gbej

Campaign's GA Account ID: UA-12798017-1

806



Domain name reconnaissance:

wh0prof.uni.me - 192.157.201.42

Known to have responded to the same IP are also the following domains:

cracks4free.info

pr0lotra.p9.org

Google Docs Hosted PUA URLs:

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCqWwqVFijUDbnTjFHdVE &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCqWwqRXBMLWZ4cVZJV2s &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCqWwqUjllLWc4MVFRQUk &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCqWwqOXlyNko0VFBOdnM &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCqWwqZm5yeUFudFhqclU &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCqWwqbWpfNW5FalJmRGM &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCqWwqS3V1ZkZBQjjGbjQ &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCqWwqX2xXbEJLbEY0Q3M &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCqWwqMU5RVkjSWURxME0 &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCqWwqVFijUDbnTjFHdVE &export=download

Dropbox Firefox Add-on/Android APK Hosted URLs:

*hxxps://dl.dropboxusercontent.com/s/so3vm50w298qkto/W
hoViewsYourProfil e.apk*

*hxxps://dl.dropboxusercontent.com/s/kor9c2mqv49esva/kka
dobe-ff.xpi*

807



Detection rate for the served PUAs, the Android adware and the rogue Firefox Add-on:

[2]MD5:

c7fcf7078597ea752b8d54e406c266a7 - detected by 5
out of 48 antivirus scanners as

PUP.Optional.CrossRider

[3]MD5: 30cf98d7dc97cae57f8d72487966d20b -
detected by 6 out of 48 antivirus scanners as
Trojan.Dropper.FB

[4]MD5:

f2459b6bde1d662399a3df725bf8891b - detected by 13
out of 48 antivirus scanners as Ad-

ware/AirPush!Android; Android Airpush;
Adware/ANDR.Airpush.G.Gen

[5]MD5:

3fb95e1ed77d1b545cf7385b4521b9ae - detected by 18
out of 48 antivirus scanners as

JS/TrojanClicker.Agent.NDL

Once executed **MD5:**

30cf98d7dc97cae57f8d72487966d20b phones back to 195.167.11.4.

Time to (conservatively) assess the campaign's damage over the year(s):

808



809



The click-through rate should be considered conservative, and it remains unknown whether the URL shortening

service was used by the cybercriminal(s) since day one of the campaign.

810



The campaign remains active, and is just the tip of the iceberg in terms of similar campaigns tricking Facebook's

users into thinking that they can eventually see who's viewed their profile. Facebook users who stumble across such

campaigns on their own, or their friends' Walls, are advised [6]**to consider reporting the campaign back to**

Facebook, immediately.

1. <http://www.webroot.com/blog/tag/pua/>

2. <https://www.virustotal.com/en/file/ecd6bb6e53477496ea45de362012b4b1d458ee966867eb89ea4005c5bd9fe8b3/analysis/1385988722/>

[is/1385988722/](https://www.virustotal.com/en/file/ecd6bb6e53477496ea45de362012b4b1d458ee966867eb89ea4005c5bd9fe8b3/analysis/1385988722/)

3. <https://www.virustotal.com/en/file/b44aabb0e235d36377f3cd55ec4af596a89c0a7814103369d3f48d54d29ffcc7/analysis/1385988808/>

[is/1385988808/](https://www.virustotal.com/en/file/b44aabb0e235d36377f3cd55ec4af596a89c0a7814103369d3f48d54d29ffcc7/analysis/1385988808/)

4. <https://www.virustotal.com/en/file/72f3834e9c8ee164b7e82383415da822579ffb23fbfa7f55ac650a22b2386ee0/analysis/1386108420/>

[is/1386108420/](https://www.virustotal.com/en/file/72f3834e9c8ee164b7e82383415da822579ffb23fbfa7f55ac650a22b2386ee0/analysis/1386108420/)

5. <https://www.virustotal.com/en/file/3b25b67592b9b06fca05ab61abd16559e7c94f9ac3c225e5ae00ddc5318923c6/analysis/1386109278/>

[811](https://www.virustotal.com/en/file/3b25b67592b9b06fca05ab61abd16559e7c94f9ac3c225e5ae00ddc5318923c6/analysis/1386109278/)

[is/1386109278/](https://www.virustotal.com/en/file/3b25b67592b9b06fca05ab61abd16559e7c94f9ac3c225e5ae00ddc5318923c6/analysis/1386109278/)

6. <https://www.facebook.com/help/www/117257561692875>

812



Continuing Facebook "Who's Viewed Your Profile" Campaign Affects Another 190k+ Users, Exposes Malicious Cybercrime Ecosystem (2013-12-11 05:01)

Last week, immediately after I published the initial analysis detailing [1]**a massive privacy-violating "Who's Viewed Your Profile" campaign, that was circulating across Facebook**, the cybercriminals behind it, supposedly took it offline, with one of the main redirectors now pointing to 127.0.0.1.

Not surprisingly, the primary campaign has multiple sub-campaigns still in circulation, which based on the lat-

est statistics – embedded within the campaign on the same day they supposedly shut it down – has already exposed

another 190,000+ of the social network's users – the original campaign appears to have been launched in 2011

having already exposed 800,000+ users – to more rogue, privacy violating apps – **JS.Febipos**, Mindspark Interactive

Network's **MyImageConverter** and **Trojan-Ransomer.CLE**, in this particular case.

Let's dissect the still circulating campaign, expose the entire infrastructure supporting it, establish direct con-

nections with it to related malicious campaigns, indicating that someone's either multi-tasking, or that their

malicious/fraudulent activities share the same infrastructure, provide MD5s for the currently served privacy-violating

apps, as well as list the actual – currently live – hosting locations.

813



Sample redirection chain:

hxxp://NXjXBMQ.tk/?12358289 - 93.170.52.21;

93.170.52.33 -> [hxxp://p2r0f3viewer9890.co.nf/?
sdk22222-](http://p2r0f3viewer9890.co.nf/?sdk22222-)

222222222222222222222222222222

~~~~~  
~~~~~

~~~~~  
~~~~~

[illegible][illegible]

~~~~~  
~~~~~

[illegible][illegible]

wh0stalks.uni.me - 192.157.201.42

cracks4free.info - 192.157.201.42

Known to have responded to 93.170.52.21 are also the following fraudulent domains:

0.facebook.com.fpama.tk

001200133184123129811.tk

00wwwebhost.tk

01203313441.tk

01prof86841.tk

029m821t9fs.4ieiit.tk

031601.tk

0333.tk

0571baidu.tk

05pr0f1le21200.tk

05pr0file214741.tk

060uty80w.tk

06emu.tk

0886.tk

0akleycityn.tk

0ao0grecu.tk

0fcf7.chantaljltaste.tk

0lod1lmt1.tk

0love.tk

The following malicious MD5s are also known to have phoned back to 93.170.52.21 in the past:

MD5: ee78fe57ad8dbac96b31f41f77eb5877

MD5: bed006372fc76ec261dc9b223b178438

MD5: 58f9cbec80d1dc3a5afbb7339d200e66

MD5: fd0c6b284f7700d59199c55fdcd5bd8a

MD5: 4bfeb3c882d816d37c3e6cbb749e44af

MD5: 97ec866ac26e961976e050591f49fec3

MD5: aba1720b1a6747de5d5345b5893ba2f5

MD5: de5e1f6f137ecb903a018976fc04e110

MD5: a9669b65cabd6b25a32352ccf6c6c09a

MD5: 003f4d9dafba9ee6e358b97b8026e354

MD5: bab313e031b0c54d50fd82d221f7defc

MD5: e6b766f627b91fd420bd93fab4bc323f

MD5: d63656d9b051bf762203b0c4ac728231

MD5: 935440d970ee5a6640418574f4569dab

MD5: 2524e3b4ed3663f5650563c1e431b05c

MD5: f726646a41f95b12ec26cf01f1c89cf9

MD5: a5af6c04d28fcea476827437caf4c681

MD5: c7346327f86298fa5dad160366a0cf26

MD5: 912ed9ef063ae5b6b860fd34f3e8b83a

MD5: b33aaa98ad706ced23d7c64aed0fcad6

815

Known to have responded to 93.170.52.33 are also the following fraudulent domains:

0lwwa.tk

0msms.tk

122.72.0.7sierra-web-www.szjlc-pcb.tk

1z8dz.tk

4f1wz8.ga

777898.ga

888234.ml

8eld7.tk

abmomre.tk

accountupdateinformation.tk

ahram-org-eg.tk

alex-fotos.tk

allycam.tk

amerdz.ml

angelsmov.tk

apis-drives-google.tk

apis-googledrive.tk

apple-idss.tk

appleid.apple.com.cgi-bin.myappleid.woa.apple-idss.tk

avtoshina.tk

The following malicious MD5s are also known to have phoned back to 93.170.52.33 in the past:

MD5: 2d951e649a8bbcbfa468f7916e188f9f

MD5: dbe2c0788e74916eba251194ef783452

MD5: 4bfeb3c882d816d37c3e6cbb749e44af

MD5: dc01c1db51e26b585678701a64c94437

MD5: 61cc3de4e9a9865e0d239759ed3c7d5a

MD5: 64505b7ca1ce3c1c0c4892abe8d86321

MD5: 0b98356395b2463ea0f339572b9c95ef

MD5: 9e87c189d3cbf2fc2414934bef6e661b

MD5: 48964a66bdc81b48f2fe7a31088c041b

MD5: f81c85bea0e2251655b7112b352f302e

The following MD5s are also known to have phoned back to 83.125.22.192 in the past:

MD5: 3935b6efa7e5ee995f410f4ef1e613ab

MD5: 64c1496e1ba2b7cb5c54a33c20be3e95

MD5: 08f76a1ed5996d7dfdcf8226fe3f66b9

MD5: f508d8034223c4ce233f1bdbed265a3a

Known to have responded to 82.208.40.11 are the following fraudulent domains:

000e0062fb44cd5b277591349e070277.cz.cc

003bc1b16c548efbc4f30790e0bc17be.cz.cc

0057ab88a8febe310f94107137731424.cz.cc

008447a58c242b52cb69fe7dceea9a0b.cz.cc

00a47e5e57323f23c66f2c2d5bc1debc.cz.cc

00a9a591d1e7aaf65639781bc73199d4.cz.cc

00ad3353e0ba865a521da380ba4e0cc4.cz.cc

00d55beb792962f7a04c66b85f2c6082.cz.cc

00e3b9ece447187da3f43f98ab619a28.cz.cc

816

00eb52dbc4331a64e4fd96fdca890d9c.cz.cc

00f59cfa33cd097e943a38a8f2e343ee.cz.cc

00fbdb49398f0e5fd9d5572044d8934e.cz.cc

010ab81241856dfca44dd9ade4489fbc.cz.cc

011622fb7752328ebb60bd2c075f1fe6.cz.cc

011fbf88cff1c18e05c2afb53d6e5ffd.cz.cc

0133147433aeef23bbe60df0cbc4eac9.cz.cc

013f98b7157ae3754d463e9d2346a549.cz.cc

013fa3e9db6e476282b8e9f1bac6d68e.cz.cc

017c2bd33744c2d423a2a7598a0c0a4e.cz.cc

019368b1f3b364c0d3ec412680638f04.cz.cc

The following malicious MD5s are also known to have phoned back to 82.208.40.11 in the past:

MD5: 2c89dfc1706b31ba7de1c14e229279e5

MD5: 6719d3e8606d91734cde25b8dfc4156f

MD5: 61dcea6fbf15b68be831bff8c5eb0c1d

MD5: 3875fa91f060d02bddd43ff8e0046588

MD5: 929b72813bae47f78125ec30c58f3165

MD5: 96fa2ea6db2e4e9f00605032723e1777

MD5: c46968386138739c81e219da6fb3ead5

MD5: 3d627e0dbc5ac51761fa7cc7b202ec49

MD5: d9714a0f7f881d3643125aa0461a30be

MD5: 81171015a95073748994e463142ddcc7

Known to have responded to 192.157.201.42 are also the following fraudulent domains:

cracks4free.info

pr0lotra.p9.org

prostats.vf1.us

wh0prof.uni.me

cracks4free.info

Time to provide the actual, currently live, hosting locations for the served privacy-violating content.

817



Mindspark Interactive Network's MyImageConverter served URL:

hxxp://download.myimageconverter.com/index.jhtml?
partner=^AZ 0^x dm081

Google Store served URLs:

hxxps://chrome.google.com/webstore/detail/miapmjacmjon
mofofflhnbaftpbfapac - currently active

hxxps://chrome.google.com/webstore/detail/dllaajjfgpigkebl
mlbamflggfjkgbej

Dropbox Accounts serving the Android app (offline due to heavy usage), and the Firefox extension:

hxxps://dl.dropboxusercontent.com/s/rueyn3owrrpsbw4/who
views5.xpi - currently online

hxxps://dl.dropboxusercontent.com/s/so3vm50w298qkto/W
hoViewsYourProfile.apk

818



Facebook App URL:

hxxp://apps.facebook.com/dislike___button/

Google Docs served privacy-violating apps:

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-
mKCuQwqVFIjUDBnTjFHdVE &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-
mKCuQwqRXBMLWZ4cVZJV2s &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-
mKCuQwqOXIyNko0VFB0dnM &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-
mKCuQwqZm5yeUFudFhqclU &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-
mKCuQwqbWpfNW5FalJmRGM &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-
mKCuQwqS3V1ZkZBQjJGbjQ &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-
mKCuQwqX2xXbEJLbEY0Q3M &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqMU5RVkjSWURxME0 &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqVFIjUDBnTjFHdVE &export=download

GA Account IDs: UA-23441223-3; UA-12798017-1

MyImageConverter Affiliate Network ID:

^AZ0^xdm081

Detection rate for the served apps/extensions:

[2]**MD5: 30cf98d7dc97cae57f8d72487966d20b** - detected by 19 out of 49 antivirus scanners as Trojan-Ransomer.CLE;

Troj/Mdrop-FNZ

[3]**MD5: 88dd376527c18639d3f8bf23f77b480e** - detected by 8 out of 49 antivirus scanners as JS:Febipos-N [Trj];

JS/Febipos

819



Once executed, **MD5:**

30cf98d7dc97cae57f8d72487966d20b also drops **MD5: 106320fc1282421f8f6cf5eb0206abee**

and **MD5: 43b20dc1b437e0e3af5ae7b9965e0392** on the affected hosts. It then phones back to 195.167.11.4:

Two more MD5s from different malware campaigns, are known to have phoned back to 195.167.11.4:

MD5: 8192c574b8e96605438753c49510cd97

MD5: d55de5e9ec25a80ddfecfb34d417b098

The Privacy Policy (<http://prostats.vf1.us/firefox/pp.html>) and the EULA (<http://prostats.vf1.us/firefox/eula.html>) point to <http://dislikeit.com> - 176.74.176.179. Not surprisingly, multiple malicious MD5s are also known to have

previously interacted with the same IP:

MD5: d366088e4823829798bd59a4d456a3df

820



MD5: 3c73db8202d084f33ab32069f40f58c8

MD5: d7fce1ec777c917f72530f79363fc6d3

MD5: 83568d744ab226a0642233b93bfc7de6

MD5: c84b1bd7c2063f34900bbc9712d66e0f

MD5: 58baa919900656dacaf39927bb614cf1

MD5: a86e97246a98206869be78fd451029a0

MD5: 70a0894397ac6f65c64693f1606f1231

MD5: f9166237199133b24cd866b61d0f6cca

MD5: 0f24ad046790ee863fd03d19dbba7ea5

Based on the latest performance metrics for the campaign, over 190,000 users have already interacted with this

sub-campaign, since 4th of December, when I initially analyzed the primary campaign.

821



Monitoring of the campaign is naturally in progress. Updates will be posted as soon as new developments take place.

This post has been reproduced from [4]Dancho Danchev's blog . Follow him [5]on Twitter.

1. <http://ddanchev.blogspot.com/2013/12/facebook-circulating-whos-viewed-your.html>
2. <https://www.virustotal.com/en/file/b44aabb0e235d36377f3cd55ec4af596a89c0a7814103369d3f48d54d29ffcc7/analysis/1386720892/>
3. <https://www.virustotal.com/en/file/4106e0e655822060a3dc83777aa88554c4f6e295b1f9474400d4820bd8e0d57b/analysis/1386720902/>
4. <http://ddanchev.blogspot.com/>
5. <http://twitter.com/danchodanchev>

822



Continuing Facebook "Who's Viewed Your Profile" Campaign Affects Another 190k+ Users, Exposes Ma-

icious Cybercrime Ecosystem (2013-12-11 05:01)

Last week, immediately after I published the initial analysis detailing [1]**a massive privacy-violating "Who's Viewed Your Profile" campaign, that was circulating across Facebook**, the cybercriminals behind it, supposedly took it offline, with one of the main redirectors now pointing to 127.0.0.1.

Not surprisingly, the primary campaign has multiple sub-campaigns still in circulation, which based on the lat-

est statistics - embedded within the campaign on the same day they supposedly shut it down - has already exposed

another 190,000+ of the social network's users - the original campaign appears to have been launched in 2011

having already exposed 800,000+ users - to more rogue, privacy violating apps - **JS.Febipos**, Mindspark Interactive

Network's **MyImageConverter** and **Trojan-Ransomer.CLE**, in this particular case.

Let's dissect the still circulating campaign, expose the entire infrastructure supporting it, establish direct con-

nections with it to related malicious campaigns, indicating that someone's either multi-tasking, or that their

malicious/fraudulent activities share the same infrastructure, provide MD5s for the currently served privacy-violating

apps, as well as list the actual - currently live - hosting locations.

823



Sample redirection chain:

hxxp://NXJXBMQ.tk/?12358289 - 93.170.52.21;

93.170.52.33 -> [hxxp://p2r0f3rviewer9890.co.nf/?
sdk22222-](http://p2r0f3rviewer9890.co.nf/?sdk22222-)

22222222222222222222222222222222
222

[illegible][illegible][illegible][illegible]

*22
222222222222222222222222 22222222222222*

~~~~~  
~~~~~

~~~~~

*22222222222222222222222222222222222222222222  
222222222222222222222222 22222222222222*







00webhost.tk

01203313441.tk

01prof86841.tk

029m821t9fs.4ieiii.tk

031601.tk

0333.tk

0571baidu.tk

05pr0f1le21200.tk

05pr0file214741.tk

060uty80w.tk

06emu.tk

0886.tk

0akleycityn.tk

0ao0greco.tk

0fcf7.chantaljtaste.tk

0lod1lmt1.tk

0love.tk

**The following malicious MD5s are also known to have phoned back to 93.170.52.21 in the past:**

MD5: ee78fe57ad8dbac96b31f41f77eb5877

MD5: bed006372fc76ec261dc9b223b178438

MD5: 58f9cbec80d1dc3a5afbb7339d200e66

MD5: fd0c6b284f7700d59199c55fdcd5bd8a

MD5: 4bfeb3c882d816d37c3e6cbb749e44af

MD5: 97ec866ac26e961976e050591f49fec3

MD5: aba1720b1a6747de5d5345b5893ba2f5

MD5: de5e1f6f137ecb903a018976fc04e110

MD5: a9669b65cabd6b25a32352ccf6c6c09a

MD5: 003f4d9dafba9ee6e358b97b8026e354

MD5: bab313e031b0c54d50fd82d221f7defc

MD5: e6b766f627b91fd420bd93fab4bc323f

MD5: d63656d9b051bf762203b0c4ac728231

MD5: 935440d970ee5a6640418574f4569dab

MD5: 2524e3b4ed3663f5650563c1e431b05c

MD5: f726646a41f95b12ec26cf01f1c89cf9

MD5: a5af6c04d28fcea476827437caf4c681

MD5: c7346327f86298fa5dad160366a0cf26

MD5: 912ed9ef063ae5b6b860fd34f3e8b83a

MD5: b33aaa98ad706ced23d7c64aed0fcad6

**Known to have responded to 93.170.52.33 are also the following fraudulent domains:**

0lwwa.tk

0msms.tk

122.72.0.7sierra-web-www.szjlc-pcb.tk

1z8dz.tk

4f1wz8.ga

777898.ga

888234.ml

8eld7.tk

abmomre.tk

accountupdateinformation.tk

ahram-org-eg.tk

alex-fotos.tk

allycam.tk

amerdz.ml

angelsmov.tk

apis-drives-google.tk

apis-googledrive.tk

apple-idss.tk

appleid.apple.com.cgi-bin.myappleid.woa.apple-idss.tk

avtoshina.tk

**The following malicious MD5s are also known to have phoned back to 93.170.52.33 in the past:**

MD5: 2d951e649a8bbcbfa468f7916e188f9f

MD5: dbe2c0788e74916eba251194ef783452

MD5: 4bfeb3c882d816d37c3e6cbb749e44af

MD5: dc01c1db51e26b585678701a64c94437

MD5: 61cc3de4e9a9865e0d239759ed3c7d5a

MD5: 64505b7ca1ce3c1c0c4892abe8d86321

MD5: 0b98356395b2463ea0f339572b9c95ef

MD5: 9e87c189d3cbf2fc2414934bef6e661b

MD5: 48964a66bdc81b48f2fe7a31088c041b

MD5: f81c85bea0e2251655b7112b352f302e

**The following MD5s are also known to have phoned back to 83.125.22.192 in the past:**

MD5: 3935b6efa7e5ee995f410f4ef1e613ab

MD5: 64c1496e1ba2b7cb5c54a33c20be3e95

MD5: 08f76a1ed5996d7dfdcf8226fe3f66b9

MD5: f508d8034223c4ce233f1bdbed265a3a

**Known to have responded to 82.208.40.11 are the following fraudulent domains:**

000e0062fb44cd5b277591349e070277.cz.cc

003bc1b16c548efbc4f30790e0bc17be.cz.cc

0057ab88a8febe310f94107137731424.cz.cc

008447a58c242b52cb69fe7dceea9a0b.cz.cc

00a47e5e57323f23c66f2c2d5bc1debc.cz.cc

00a9a591d1e7aaf65639781bc73199d4.cz.cc

00ad3353e0ba865a521da380ba4e0cc4.cz.cc

00d55beb792962f7a04c66b85f2c6082.cz.cc

00e3b9ece447187da3f43f98ab619a28.cz.cc

826

00eb52dbc4331a64e4fd96fdca890d9c.cz.cc

00f59cfa33cd097e943a38a8f2e343ee.cz.cc

00fbdb49398f0e5fd9d5572044d8934e.cz.cc

010ab81241856dfca44dd9ade4489fbc.cz.cc

011622fb7752328ebb60bd2c075f1fe6.cz.cc

011fbf88cff1c18e05c2afb53d6e5ffd.cz.cc

0133147433aeef23bbe60df0cbc4eac9.cz.cc

013f98b7157ae3754d463e9d2346a549.cz.cc

013fa3e9db6e476282b8e9f1bac6d68e.cz.cc

017c2bd33744c2d423a2a7598a0c0a4e.cz.cc

019368b1f3b364c0d3ec412680638f04.cz.cc

**The following malicious MD5s are also known to have phoned back to 82.208.40.11 in the past:**

MD5: 2c89dfc1706b31ba7de1c14e229279e5

MD5: 6719d3e8606d91734cde25b8dfc4156f

MD5: 61dcea6fbf15b68be831bff8c5eb0c1d

MD5: 3875fa91f060d02bddd43ff8e0046588

MD5: 929b72813bae47f78125ec30c58f3165

MD5: 96fa2ea6db2e4e9f00605032723e1777

MD5: c46968386138739c81e219da6fb3ead5

MD5: 3d627e0dbc5ac51761fa7cc7b202ec49

MD5: d9714a0f7f881d3643125aa0461a30be

MD5: 81171015a95073748994e463142ddcc7

**Known to have responded to 192.157.201.42 are also the following fraudulent domains:**

cracks4free.info

pr0lotra.p9.org

prostats.vf1.us


wh0prof.uni.me

cracks4free.info

Time to provide the actual, currently live, hosting locations for the served privacy-violating content.

827

*... the only truly working solution approved by facebook community! Try it! Share it!*



The image is a screenshot of a Facebook advertisement for a browser extension. At the top left is a magnifying glass icon over a person's silhouette. To its right is the title "Who Viewed Your Profile" in a large, bold font, followed by the subtitle "More ways to experience Facebook" in a smaller font. Below the title is a horizontal line. To the left of this line is the text "Introducing the new 'Who Viewed Your Profile' feature on facebook!" in bold. Below this is a paragraph: "Ever wanted to see how views your profile? on Facebook? Now you can! Let yourself do it already! It's Just an Extension to install." To the right of the text is a screenshot of the Facebook interface showing a sidebar menu with options: News Feed, Messages, Events, Photos, Friends, Who's Viewed me (59), Applications, and Games. A large red arrow points to the "Who's Viewed me (59)" option. Below the sidebar is a blue button with the word "facebook" in white. At the bottom of the advertisement is a green button with the word "INSTALL" in white.

**Mindspark Interactive Network's MyImageConverter served URL:**

hxxp://download.myimageconverter.com/index.jhtml?  
partner=^AZ 0^xdm081

**Google Store served URLs:**



hxxps://chrome.google.com/webstore/detail/miapmjacmjonm  
ofofflhnbaftpbfapac - currently active

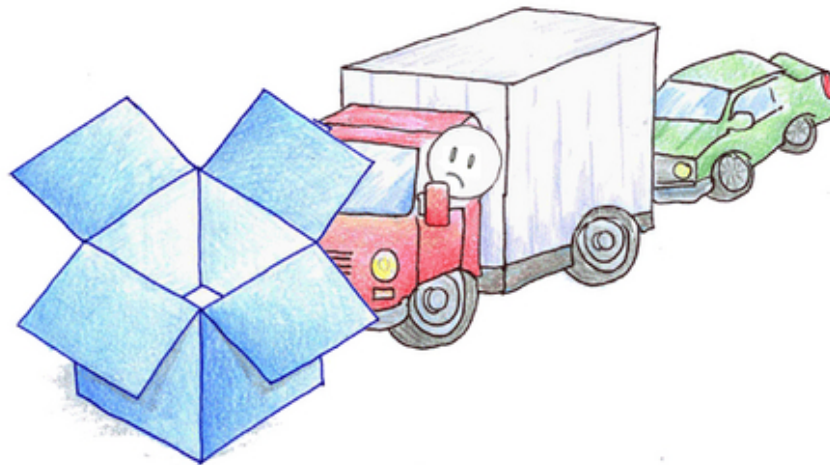
hxxps://chrome.google.com/webstore/detail/dllaajjfgpigkebl  
mlbamflggfjkgbej

**Dropbox Accounts serving the Android app (offline  
due to heavy usage), and the Firefox extension:**

hxxps://dl.dropboxusercontent.com/s/rueyn3owrrpsbw4/who  
views5.xpi - currently online

hxxps://dl.dropboxusercontent.com/s/so3vm50w298qkto/Wh  
oViewsYourProfile.apk

828



**Error (509)**

This account's public links are generating too much traffic and have been temporarily disabled!

## **Facebook App URL:**

hxxp://apps.facebook.com/dislike\_\_\_button/

## **Google Docs served privacy-violating apps:**

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqVFIjUDBnTjFHdVE &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqRXBMLWZ4cVZJV2s &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqOXIyNko0VFBOdnM &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqZm5yeUFudFhqclU &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqbWpfNW5FaljmRGM &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqS3V1ZkZBQjJGbjQ &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqX2xXbEJLbEY0Q3M &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqMU5RVkJSWURxME0 &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqVFIjUDBnTjFHdVE &export=download

**GA Account IDs:** UA-23441223-3; UA-12798017-1

## **MyImageConverter Affiliate Network ID:**

^AZ0^x dm081

## **Detection rate for the served apps/extensions:**

**[2]MD5: 30cf98d7dc97cae57f8d72487966d20b** - detected by 19 out of 49 antivirus scanners as Trojan-Ransomer.CLE;

Troj/Mdrop-FNZ

**[3]MD5: 88dd376527c18639d3f8bf23f77b480e** - detected by 8 out of 49 antivirus scanners as JS:Febipos-N [Trj];

JS/Febipos

829

## Privacy Policy

This policy describes how and why DislikeIt LLC, Incorporated in the United States ("dba DislikeIt") collects non-personally identifiable data from users and website visitors to DislikeIt's website (DislikeIt.com), and how that data will be used. DislikeIt is committed to respecting the privacy of non-personal identifiable data gathered.

### Use of Data

DislikeIt uses non-personally identifiable data collected from users and website visitors in order to:

- To improve the quality and functionality of the Software and the website, to enhance your experience, to create new services, including customized services, to change or cancel existing content or services and for other internal and statistical purposes;
- To present you relevant content, marketing materials and advertisements, by analyzing your interests from the web pages and you visit and online services that you use;
- To provide you with support and handle inquiries;
- To enforce the Software EULA;
- To comply with any applicable law and assist law enforcement agencies as required;
- To conduct surveys and market researches;
- We may use anonymous, statistical or aggregated information about the Software's use and share, publish, post, disseminate, transmit or otherwise communicate or make available such information, to suppliers, business partners, sponsors, affiliates and any other third party, at our sole discretion.

### Cookies and Log Files

Cookies may be used on some pages of our site. Cookies are small text files placed on your hard drive that assist us in providing a more customized website experience. It is DislikeIt's policy to use cookies to make navigation of our website easier for visitors. If you are concerned about cookies, most browsers permit individuals to decline cookies. A user refusing cookies can still fully navigate our website. In order to properly manage our website we may anonymously log information on our systems, and identify categories of visitors by items such as domains and browser types. These statistics are used to manage the operational efficiency of our systems.

### Age Limit

We never knowingly collect or maintain information at or on our website from those we actually know are under 18, and no part of our website is directed at or structured to attract anyone under 18. Visitors younger than 18 years of age may NOT use the Site and the Software and must LEAVE immediately.

### Changes to Policy

From time to time, we may revise this policy and we will post the revised Policy on the Site. Therefore, it is recommended that you read it periodically. All substantial changes made to this policy will be notified on the Site, at our sole discretion, and will take effect immediately.

### Governing Law

This Privacy Policy is governed by and construed in accordance with the laws of the United States. You agree to submit any dispute arising out of your use of this Web site to the exclusive jurisdiction of the courts of THE UNITED STATES.

### Contact us

Please direct all questions in connection with this Policy via e-mail to: [info@http://DislikeIt.com/](mailto:info@http://DislikeIt.com/)

Once executed, **MD5:**

**30cf98d7dc97cae57f8d72487966d20b** also drops **MD5:**  
**106320fc1282421f8f6cf5eb0206abee**

and **MD5: 43b20dc1b437e0e3af5ae7b9965e0392** on  
the affected hosts. It then phones back to 195.167.11.4:

**Two more MD5s from different malware campaigns,**  
**are known to have phoned back to 195.167.11.4:**

MD5: 8192c574b8e96605438753c49510cd97

MD5: d55de5e9ec25a80ddfecfb34d417b098

The Privacy Policy ( <http://prostats.vf1.us/firefox/pp.html>) and the EULA ( <http://prostats.vf1.us/firefox/eula.html>) point to <http://dislikelt.com> - 176.74.176.179. Not surprisingly, multiple malicious MD5s are also known to have

previously interacted with the same IP:

MD5: d366088e4823829798bd59a4d456a3df

830

## End User License Agreement

PLEASE TO USER THIS END-USER LICENSE AGREEMENT ("EULA" "AGREEMENT") APPLIES WITH RESPECT TO SOFTWARE APPLICATIONS AND DIGITAL CONTENT OWNED AND PROVIDED BY Dellware, AND ITS SUBSIDIARIES (REFERRED TO IN THIS AGREEMENT AS "Dellware") FROM OUR Dellware WEBSITE. THIS AGREEMENT SETS FORTH YOUR RIGHTS AND OBLIGATIONS WITH RESPECT TO YOUR USE OF ANY Dellware SOFTWARE ("SOFTWARE"), BUT SHALL NOT GOVERN YOUR USE OF ANY THIRD PARTY SOFTWARE. PLEASE READ THIS AGREEMENT CAREFULLY BY CLICKING "ACCEPT," "YIKES!" "CONTINUE" OR A SIMILAR ACKNOWLEDGMENT BEFORE, OR IN USING ALL OR ANY PORTION OF THE SOFTWARE. YOU ACCEPT ALL THE TERMS AND CONDITIONS OF THIS AGREEMENT. YOU AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU. IF YOU DO NOT AGREE, DO NOT INSTALL OR USE THE SOFTWARE.

**3. Definitions.** "Software" means (a) the Inflight, or any other software or digital content owned and provided by Inflight, that accompanies this Agreement, and its any bug fixes, upgrades, modified versions or updates to the Software (collectively referred to as "Updates"); that Inflight subsequently provides to you. "Use," "Used" or "Using" means to access, install, download, copy or benefit from utilizing the functionality of the Software.

**2. Age Limitation.** You must be at least 18 years of age to use the Software. By accepting the terms of this Agreement and using the Software, you represent that you are over the age of 18. As long as you comply with, and adhere to, the terms of this Agreement, DellSoft grants to you a non-exclusive, revocable, limited license to download and install the most current generally available version of the Software, in binary executable form only, solely for the purposes described in this Agreement.

**3. Other Software.** In addition to the Software, you will also be given the opportunity to access, download and/or use the technologies, services and/or content owned by third parties collectively, "Other Software". If you choose to access or use such Other Software, you acknowledge and agree that your rights to such Other Software are governed solely by the license terms and conditions accompanying the Other Software. For example, you may be required to click and accept additional end user license agreements ("EULAs") prior to the download, installation, or use of such Other Software. If such EULA grants you any use of Other Software, you agree to the terms of this Agreement. However, such Other EULA shall not affect any terms in this Agreement or your use of the Software. You further agree that Dribbble is not responsible for any loss or damage of any sort incurred as a result of your download, installation, or use of Other Software, and you hereby waive and hold Dribbble harmless from any losses arising under any claim you may have against Dribbble with respect to Other Software.

4. **Restrictions.** You will (a) not reverse engineer, disassemble or decompile the Software or attempt to discover or recreate the source code to the Software, except as otherwise required by applicable law; (b) comply with all applicable laws, including U.S. export control laws, in your use of the Software; (c) not make any modifications, adaptation, improvement, enhancement, translation or derivative work of or to the Software; (d) not remove, alter or obscure any proprietary notice including copyright notice(s) of Delltek or its licensors in the Software; (e) not use the Software for purposes for which it is not designed; and (f) only use the Software for personal, non-commercial use.

**5. Intellectual Property Rights.** The Software is the intellectual property of, and owned by Delland and its licensors and suppliers. The structure, organization and code of the Software are the valuable trade secrets and confidential information of Delland and its licensors and suppliers. The Software is protected by state, federal and international copyright protections, including without limitation by the United States copyright law, international treaty provisions and applicable laws in the country in which it is being used. Except as expressly stated herein, the Agreement does not grant you any intellectual property rights in the Software by implication, estoppel or any other legal theory, and all rights not expressly granted in the Agreement are reserved to Delland and its agents, licensors and suppliers.

**6. Third Party Software, Notice and Attribution.** The Software may include third party's software located subject to open source or third party license terms. You acknowledge and agree that your right to use those publicly available components of the Software is governed by the terms applicable to such application ("Other Software Terms"). In the event of any conflict with the express terms of this Agreement and the Other Software Terms, the Other Software Terms of such publicly available license shall control your use of the relevant application.

7. **Display of suggested search results.** By installing and/or using the software you grant Dailidat permission to periodically show you search sites based on your activity. To display the search ads, the user must click on the keyword search on the search result page for example click on [HTTP://www.Dailidat.com/links.htm](http://www.Dailidat.com/links.htm). Dailidat will display enhanced search results including organic and sponsored ads with Google Search Results, Youtube Video Results, Bing Search Results and also has an option to view similar sites for the keyword search term.

You hereby consent to these actions. Please note that you may receive search results for adult-oriented websites if you utilize keywords connected to, search for or view adult websites. An adult website is one that contains or references (whether by audio, video, endorsement, images, sounds or text) any of the following profanity, violence, blood and gore, weapons, use of alcohol, drugs, tobacco, online gambling, pornography, erotica, erotic images, nudity, sex, sexually explicit images, and sexual references. All search results are derived from third parties and Dailymile, as much as we can, take responsibility for transactions done with the third party websites. However, if any of the search results breach local laws please advise Dailymile immediately via [DP@Dailymile.COM](mailto:DP@Dailymile.COM).

**8. Uninstallation.** You understand and agree that the presence of the Software on your computer is voluntary and that you may remove the Software from your computer at any time. The Software may be uninstalled by clicking to the "Uninstall link" at the bottom of the main homepage page and following instructions on your computer. For specific uninstall instructions, go to <http://www.judicial.com/onlinehelp.html>.

**8. Updates.** Dribbble, in its sole discretion, may provide you with Updates to the Software as part of this Agreement. The Software will automatically check with Dribbble servers for the existence of any Updates that have been released, and in the event that one is available, the Software will update itself automatically. Nothing herein shall be construed as or interpreted as requiring Dribbble to provide Updates. Dribbble will not install any new software or Updates that in Dribbble's reasonable judgment has functionality that is materially different from the functionality of the previously installed Software without your prior consent.

10. **Disclaimer of Warranties and Remedies; Indemnity.**

[illegible]

**9.3. Limitations of Damages.** NEITHER DALLAS NOR ANY OF ITS LICENSEE OR SUPPLIERS WILL BE, AND YOU RELEASE DALLAS AND ALL OF ITS LICENSEE AND SUPPLIERS FROM ANY LIABILITY (INCLUDING IN CONTRACT, WARRANTY, TORT, NEGLIGENCE OR OTHERWISE) FOR ANY DAMAGES (INCLUDING IF YOU SUFFERING FROM ANY LOSS OR INABILITY TO USE THE SOFTWARE OR ANY OTHER SOFTWARE, INCLUDING, WITHOUT LIMITATION, ANY DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, PUNITIVE, OR EXEMPLARY DAMAGES) OF ANY KIND OR LOSS OF PROFITS, DATA, OR GOODWILL, EVEN IF DALLAS OR ANY OF ITS LICENSEE OR SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, IN NO EVENT SHALL DALLAS OR ANY OF ITS LICENSEE OR SUPPLIERS' ENTIRE LIABILITY ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT EXCEED OR BE LIMITED TO THE AMOUNT OF THE LICENSE FEE. THE LIMITATIONS HEREIN WILL APPLY NOTWITHSTANDING THE FAILURE OF ESSENTIAL PURPOSE OF ANY LIMIT REMEDY UNDER THIS AGREEMENT.

SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES OR THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES. ACCORDINGLY, SOME OF THE ABOVE LIMITATIONS MAY NOT APPLY TO YOU. IN SUCH JURISDICTIONS, THE FOREGOING DISCLAIMERS SHALL APPLY TO THE GREATEST EXTENT PERMITTED BY APPLICABLE LAW OR SHALL BE RECONSTRUCTED TO COMPLY WITH THE DISCLAIMERS INTENT TO THE FULLEST EXTENT PERMITTED BY SUCH JURISDICTION.

Any representations made with respect to, and support or assistance offered by Daldit in connection with, the Software are offered by Daldit only and not by any third party providing open source to Daldit.

**11. Use of Information.** By installing the Software, you grant Dinkbit permission to collect and use certain information. We acknowledge that you have reviewed Dinkbit Privacy Policy, which describes Dinkbit practices with respect to the collection, use and disclosure of information in connection with your use of the Software.

**3.2. Compatibility:** Dellinet does not warrant that the Software will be compatible with your hardware or other software installed on your computer system. Compatibility issues may cause your computer's performance to suffer in the event that the Software is not compatible with your hardware or other software installed on your computer system, the Software can be uninstalled. Please refer to Section 8 (warranty) for detailed warranty details. Like all software, the Software undergoes some of your computer's resources to run, including system memory and your Internet connection. Use of the Software on a computer with inadequate system resources will cause each computer's performance to suffer.

**8.8. User Representations and Warranties.** You acknowledge, represent and warrant that (a) you own the computer on which you are installing the Software, or have the authority to install the Software on such computer; (b) your installation and/or use of the Software will not violate any local, state or federal laws that apply to you or to the Use or installation of the Software; and (c) DellNet is not causing the Software to be installed on your computer, but has provided the Software to you, which you are installing of your own volition.

**11. Indemnification.** You agree to defend, indemnify, and hold harmless Inteltek, its licensors and suppliers, and each of their respective officers, directors and employees, from and against any lawsuits, claims, losses, damages, fees and expenses (including attorney's fees and costs) arising out of your use of the Software or your breach of this Agreement.

**15. Export.** You agree that the Software may not be acquired, shipped, transported, exported, or re-exported (a) into (or to a national or resident of) any U.S. embargoed country or (b) to anyone on the U.S. Treasury Department's list of Specially Designated Nationals or the U.S. Department of Commerce's Table of Denied Orders. By using the Software, you represent and warrant that you are not located in, under control of, or a national or resident of any such country or on any such list.

**10. Governing Law; Dispute Resolution.** This agreement will be governed by and construed in accordance with the laws of the State of Illinois, without regard to its choice of law principles. Any controversy, dispute or claim arising out of or relating to this agreement, including its interpretation, validity, performance, non-performance or breach, shall be resolved by binding arbitration conducted in the UNITED STATES. The parties shall bear their own respective costs and attorneys' fees. Any award, regardless of any statute or law to the contrary, any claim or cause of action arising out of or related to use of the website, the Software, the services or this agreement must be made within one (1) year after each claim or cause of action arose or be forever barred.

**17. Miscellaneous.** This is the entire agreement between Delltek and you relating to the software, and it supersedes any prior representations, discussions, understandings, communications or advertising relating to the software. If any part of this Agreement is held by a court to be illegal, voided or unenforceable, then that provision shall be deemed severable and will not affect the validity of the balance of the Agreement, which will remain valid and enforceable according to its terms. This Agreement may only be modified by a writing signed by an authorized officer of Delltek. If you violate any term of this Agreement, Delltek may terminate this Agreement without waiving any other rights. This Agreement is assignable by Delltek but you may not assign your rights and obligations under the Agreement.

MD5: 3c73db8202d084f33ab32069f40f58c8

MD5: d7fce1ec777c917f72530f79363fc6d3

MD5: 83568d744ab226a0642233b93bfc7de6

MD5: c84b1bd7c2063f34900bbc9712d66e0f

MD5: 58baa919900656dacaf39927bb614cf1

MD5: a86e97246a98206869be78fd451029a0

MD5: 70a0894397ac6f65c64693f1606f1231

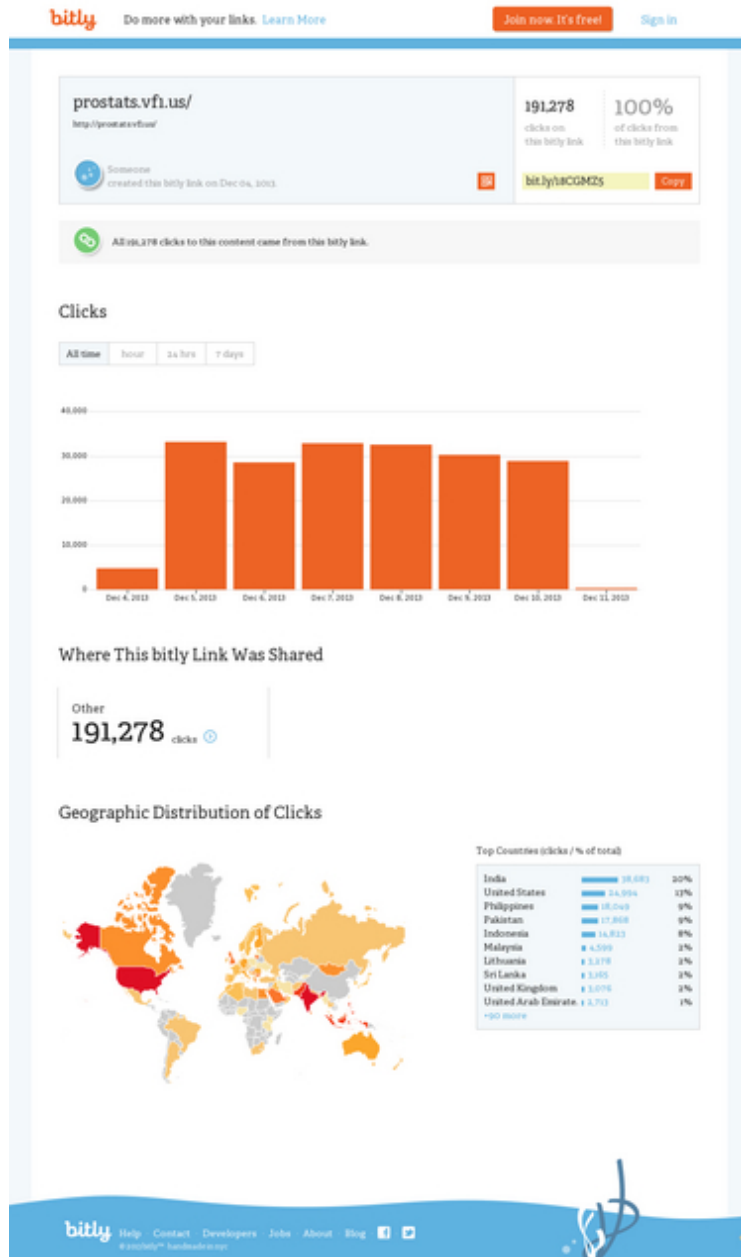
MD5: f9166237199133b24cd866b61d0f6cca

MD5: 0f24ad046790ee863fd03d19dbba7ea5

Based on the latest performance metrics for the campaign, over 190,000 users have already interacted with this

sub-campaign, since 4th of December, when I initially analyzed the primary campaign.

831



Monitoring of the campaign is naturally in progress. Updates will be posted as soon as new developments take place.

1. <http://ddanchev.blogspot.com/2013/12/facebook-circulating-whos-viewed-your.html>
2. <https://www.virustotal.com/en/file/b44aabb0e235d36377f3cd55ec4af596a89c0a7814103369d3f48d54d29ffcc7/analysis>



[is/1386720892/](#)

3.

<https://www.virustotal.com/en/file/4106e0e655822060a3dc83777aa88554c4f6e295b1f9474400d4820bd8e0d57b/analysis/1386720902/>

[is/1386720902/](#)

832

**2.**

**2014**

833

**2.1**

**January**

834

# Webroot Threat Blog

Internet Security Threat Updates & Insights

 **READ**  
Webroot Blogs

 **WATCH**  
Webroot Vlogs

 **CONNECT**  
Meet The Threat Team

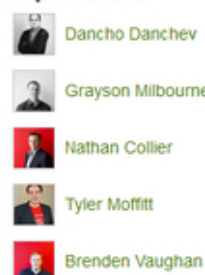
 **DISCUSS**  
Webroot Community

Search for:

## Our Extended Community



## Top Authors



## Looking For Support?

The Webroot Community is happy to answer your questions, but if you're looking for our official support department please open a

## Top consumer security predictions for 2014

December 31st, 2013 by [Tyler Moffitt](#)

Top Predictions for 2014 FBI/ICE MoneyPak Cryptolocker Rogues As this year comes to a close we've seen some measurable progress on the infiltration techniques for malware. We're going to give you some insight into some of the top threats of 2013 and what it could mean for 2014. FBI/ICE MoneyPak We saw some frightening improvements with Ransomware this year. FBI/ICE MoneyPak or Win32.Reveton was a huge hit to the PC community. Although first seen in 2012 it wasn't until 2013 that it was tweaked to be one of the most annoying and difficult Ransomware to remove. Once dropped on your [...]

[CONTINUE READING »](#)

Posted in: [FBI Ransomware](#), [spyware](#), [Threat Research](#)

Tagged: [2014 predictions](#), [consumer threats](#), [Malicious Software](#), [malware](#), [phishing](#), [predictions](#), [Threat Research](#), [vulnerabilities](#), [Webroot blog](#)

## Cybercrime Trends 2013 – Year in Review

December 27th, 2013 by [Dancho Danchev](#)

It's that time of the year! The moment when we reflect back on the cybercrime tactics, techniques and procedures (TTPs) that shaped 2013, in order to constructively speculate on what's to come for 2014 in terms of fraudulent and malicious campaigns, orchestrated by opportunistic cybercriminal adversaries across the globe. Throughout 2013, we continued to observe and profile TTPs, which were crucial for the success, profitability and growth of the cybercrime ecosystem internationally, such as, for instance, widespread proliferation of the campaigns, professionalism and the implementation of basic business/economic/marketing concepts, improved QA (Quality Assurance), vertical integration in an attempt to occupy [...]

x

## Summarizing Webroot's Threat Blog Posts for December (2014-01-06 17:07)

The following is a brief summary of all of my posts at [1]**Webroot's Threat Blog** for December, 2013. You can

subscribe to [2]**Webroot's Threat Blog RSS Feed**, or follow me on Twitter:

**01.** [3]Cybercrime-friendly VPN service provider pitches itself as being 'recommended by Edward Snowden'

**02.** [4]Commercial Windows-based compromised Web shells management application spotted in the wild

**03.** [5]Compromised legitimate Web sites expose users to malicious Java/Symbian/Android “Browser Updates”

**04.** [6]Malicious multi-hop iframe campaign affects thousands of Web sites, leads to a cocktail of client-side exploits

– part two

**05.** [7]How cybercriminals efficiently violate YouTube, Facebook, Twitter, Instagram, SoundCloud and Google+’s ToS

**06.** [8]Tumblr under fire from DIY CAPTCHA-solving, proxies-supporting automatic account registration tools

**07.** [9]Newly launched ‘HTTP-based botnet setup as a service’ empowers novice cybercriminals with bulletproof

hosting capabilities – part three

835

**08.** [10]Cybercriminals offer fellow cybercriminals training in Operational Security (OPSEC)

**09.** [11]Fake ‘WhatsApp Missed Voicemail’ themed emails lead to pharmaceutical scams

**10.** [12]A peek inside the booming underground market for stealth Bitcoin/Litecoin mining tools

**11.** [13]Cybercrime Trends 2013 – Year in Review

***This post has been reproduced from [14]Dancho Danchev’s blog . Follow him [15]on Twitter.***

1. <http://www.webroot.com/blog>
2. <http://feeds2.feedburner.com/WebrootThreatBlog>
3. <http://www.webroot.com/blog/2013/12/03/cybercrime-friendly-vpn-service-provider-pitches-recommended-edward-snowden/>
4. <http://www.webroot.com/blog/2013/12/04/commercial-windows-based-compromised-web-shells-management-application-spotted-wild/>
5. <http://www.webroot.com/blog/2013/12/05/compromised-legitimate-web-sites-expose-users-malicious-javasymbian-android-browser-updates/>
6. <http://www.webroot.com/blog/2013/12/09/malicious-multi-hop-iframe-campaign-affects-thousands-web-sites-leads-cocktail-client-side-exploits-part-two/>
7. <http://www.webroot.com/blog/2013/12/11/cybercriminals-efficiently-violate-monetize-youtube-facebook-twitter-instagram-soundcloud-googles-tos/>
8. <http://www.webroot.com/blog/2013/12/12/tumblr-fire-diy-captcha-solving-proxies-supporting-automatic-account-registration-tools/>

9. <http://www.webroot.com/blog/2013/12/16/newly-launched-http-based-botnet-setup-service-empowers-novice-cybercriminals-bulletproof-hosting-capabilities-part-three>

10.

[http://www.webroot.com/blog/2013/12/17/cybercriminals-offer-fellow-cybercriminals-training-in-operational](http://www.webroot.com/blog/2013/12/17/cybercriminals-offer-fellow-cybercriminals-training-in-operational-security-opsec/)

[-security-opsec/](http://www.webroot.com/blog/2013/12/17/cybercriminals-offer-fellow-cybercriminals-training-in-operational-security-opsec/)

11.

[http://www.webroot.com/blog/2013/12/17/cybercriminals-offer-fellow-cybercriminals-training-in-operational](http://www.webroot.com/blog/2013/12/17/cybercriminals-offer-fellow-cybercriminals-training-in-operational-security-opsec/)

[-security-opsec/](http://www.webroot.com/blog/2013/12/17/cybercriminals-offer-fellow-cybercriminals-training-in-operational-security-opsec/)

12. <http://www.webroot.com/blog/2013/12/19/peek-inside-booming-underground-market-stealth-bitcoin-litecoin-mining-tools/>

13. <http://www.webroot.com/blog/2013/12/27/cybercrime-trends-2013-year-review/>

14. <http://ddanchev.blogspot.com/>

15. <http://twitter.com/danchodanchev>



shared a link.

15 minutes ago

See also nonsense that does not follow anymore GgG these people do not pay attention to what you wear ? 9h4NcvDD27IyXWa — with [redacted] and 19 others.



Odd minutes of the live broadcast! lwJ Dress-through the difficult moments of the artist! 7QqQW vDD2

Odd minutes of the live broadcast! lwJ Dress-throu...

It does not make us images v06 First time with you! Abolition watch! T3Dp0

Like · Comment · Share

## Fake Adobe Flash Player Serving Campaign Utilizes Google Hosting/Redirection Infrastructure, Spreads

### Across Facebook (2014-01-07 21:09)

What "better" time to spread malicious "joy", then during the Holidays? Cybercriminals are still busy maintaining a fake Adobe Flash Player serving, Facebook spreading campaign, which I originally intercepted during the Holidays,

utilizing Google redirectors/hosting services. Despite the modest – naturally conservative estimate – click-through

rate (45,000 clicks) compared to that of the most recently profiled similar [1]**Febipos spreading campaign**, which

[2]**resulted in over 1 million clicks**, the campaign remains active, and continues tricking users into installing the rogue Adobe Flash Player, resulting in the continued spread of the campaign, on the Facebook Walls of socially engineered

users.

Let's dissect the campaign, expose its infrastructure/command and control servers, and provide MD5s of the served

malware.

## **Spamvertised**

### **Facebook**

#### **URL+redirection**

##### **chain:**

*hxxp://goo.gl/QeshtO;*

*hxxp://goo.gl/vVbrHp;*

*hxxp://goo.gl/0oSJ7z; hxxp://goo.gl/38qlq8;*

*hxxp://goo.gl/QNQhc5 ->*

*hxxps://9dvme0lk2r0osqg3qb3rlk95z.storage.googleapis.com/q1fwum32gld35 iab9d2u4o35bjsvhjhu309.html?ref=12 ->*

*hxxp://goo.gl/wKXme1 -> hxxp://www.i-justice.org/g-o-27312-gooenn.html*

**(94.23.166.27)**

*->*

*hxxp://f3c47a0d01f3ec343f57-*

*2ba5bba9317af81ae21c42000295a455.r9.cf4.*

*-*

*rackcdn.com/24471bmbqv07595?ref=27312*

*&aff*

*\_sub=27312*

*&sub*

*\_id=27312*

*->*

*hxxp://www.eklentidunyasi.com/dl.php (176.31.2.155) or  
hxxp://www.agentofex.com/dl.php (176.227.218.99;  
www.puee.in) ->*

*hxxp://docs.google.com/uc?export=download*

*&id=0B6DFdqpSFDAISmpsTkZkT2hvN28*

*or*

*hxxps://doc-*

*0g-4o-*

*docs.googleusercontent.com/docs/securesc/ha0ro937gcu*

*c7l7deffksulhg5h7mbp1/7fbm9gn-*

*67t8t18r8etd00juf0rvmrrmh/1387836000000/1*

*6300082901287672546/\*/0BzU3dARQGry0TIMxN3F2STN0Z3  
M*

**GA Account ID:** UA-36486228-1

837



<http://goo.gl/wKXme1>

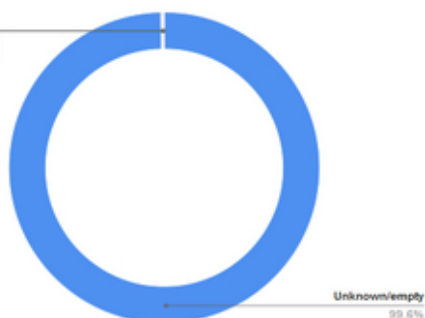
<http://www.i-justice.org/g-o-27312-gooenn.html>

Created: 2013 Dec 23

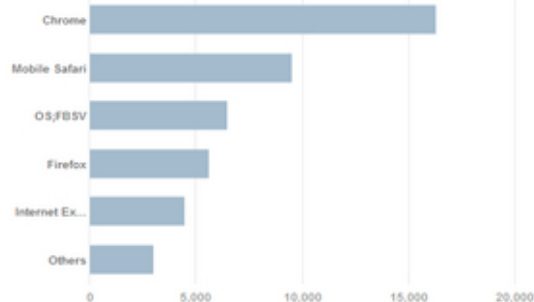


#### Referrers

Other  
0.2%  
Others  
0.2%



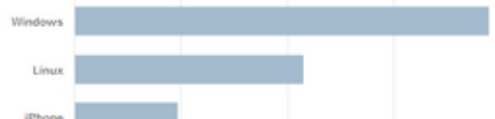
#### Browsers



#### Countries



#### Platforms



**Detection rate for the served malware: [3]MD5: 30118bec581f80de46445aef79e6cf10** - detected by 33 out of 48

antivirus scanners as Trojan-Ransom.Win32.Blocker.dbud.

Once executed, the sample phones back to:

`hxxp://176.31.2.155/extFiles/control8.txt`

`hxxp://176.31.2.155/extFiles/NewFile0008.exe`

`hxxp://176.31.2.155/extFiles/version.txt`

hxxp://176.31.2.155/extFiles/list.txt

hxxp://176.31.2.155/extFiles/list.txt

hxxp://176.31.2.155/extFiles/buflash.xpi

hxxp://176.31.2.155/extFiles/bune10.zip

hxxp://176.31.2.155/extFiles/private/sandbox\_status.php

hxxp://176.31.2.155/extFiles/extFiles/yok.txt

838

Now Page **985 people** total **3,457 video's** watched...



[register](#) [login](#)

[home](#) [category](#) [channel](#)

### Forget to wear pants, Selena Star sparks underwear riddle

Please install Flash Player...

15,547 watched

1 day ago

share: [f](#) [t](#) [in](#) [g](#)

#### Navigator

- [. home](#)
- [. about us](#)
- [. category](#)
- [. chanelis](#)
- [. faq](#)
- [. contact](#)

#### Social Newtork

- [Facebook](#)
- [Twitter](#)

© 2011 - unluvideolari.info

The files were offline in time of processing of the sample.

### **Related MD5s for the same served fake Adobe Flash Player:**

MD5: 61f5af5d0067ea8d10f0764ff3c82066

MD5: 80b9ef43183abdd5b22482bc1cea7b36

MD5: 2da7cb838234eebbca3115fcafd6f513

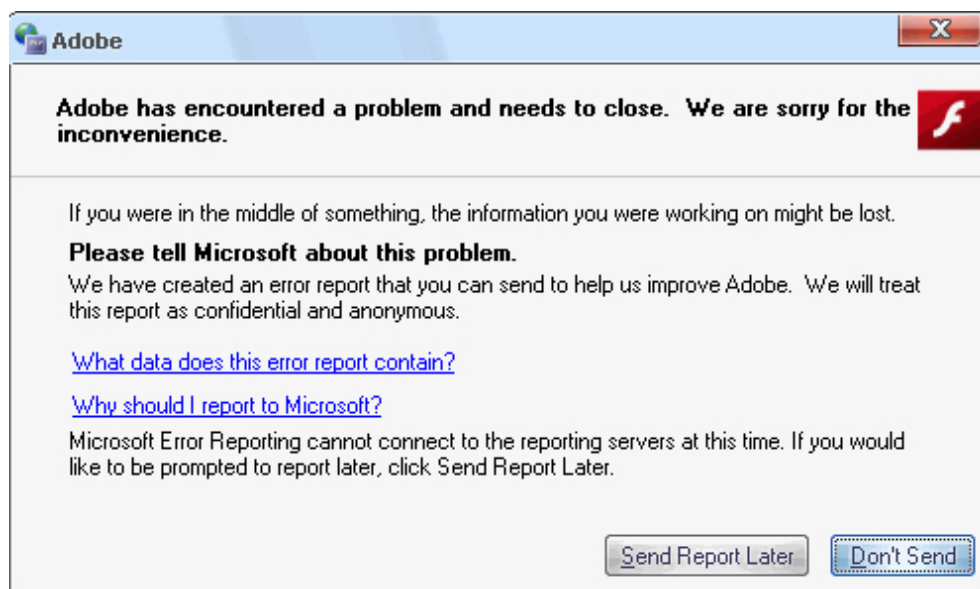
MD5: 40ae8d901102ee3951c241b394eb94e9

MD5: 30118bec581f80de46445aef79e6cf10

MD5: 2de9865032e997d59c03bfd8435f1ada

MD5: fce013bec7b3651c100b6887c0a12eee

839



**Once executed, MD5:  
fce013bec7b3651c100b6887c0a12eee phones back  
to:**

hxxp://176.227.218.99/extFiles/control17.txt

hxxp://176.227.218.99/extFiles/NewFile00017.exe

hxxp://46.163.100.240/NewFile00017.exe

hxxp://176.227.218.99/NewFile00017.exe

hxxp://176.227.218.99/extFiles/extFiles/version.txt

hxxp://176.227.218.99/extFiles/extFiles/list.txt

hxxp://176.227.218.99/extFiles/extFiles/buflash.xpi

hxxp://176.227.218.99/extFiles/extFiles/bune10.zip

Files remain offline in the time of processing of the sample.

***This post has been reproduced from [4]Dancho Danchev's blog . Follow him [5]on Twitter.***

1. <http://ddanchev.blogspot.com/2013/12/continuing-facebook-whos-viewed-your.html>

2. <http://ddanchev.blogspot.com/2013/12/facebook-circulating-whos-viewed-your.html>

3. <https://www.virustotal.com/en/file/ade1707efaa1496691d5d4b12daadff893b0f0ad68b33699e5dd7dd6f8eb58/analysis/1387838333/>

4. <http://ddanchev.blogspot.com/>

5. <http://twitter.com/danchodanchev>



shared a link.

15 minutes ago

See also nonsense that does not follow anymore GgG these people do not pay attention to what you wear ? 9h4NcvDD27IyXWa — with [redacted] and 19 others.



Odd minutes of the live broadcast! lwJ Dress-through the difficult moments of the artist! 7QqQW vDD2

Odd minutes of the live broadcast! lwJ Dress-throu...

It does not make us images v06 First time with you! Abolition watch! T3Dp0

Like · Comment · Share

## Fake Adobe Flash Player Serving Campaign Utilizes Google Hosting/Redirection Infrastructure, Spreads

### Across Facebook (2014-01-07 21:09)

What "better" time to spread malicious "joy", then during the Holidays? Cybercriminals are still busy maintaining a fake Adobe Flash Player serving, Facebook spreading campaign, which I originally intercepted during the Holidays,

utilizing Google redirectors/hosting services. Despite the modest – naturally conservative estimate – click-through

rate (45,000 clicks) compared to that of the most recently profiled similar [1]**Febipos spreading campaign**, which

[2]**resulted in over 1 million clicks**, the campaign remains active, and continues tricking users into installing the rogue Adobe Flash Player, resulting in the continued spread of the campaign, on the Facebook Walls of socially engineered

users.

Let's dissect the campaign, expose its infrastructure/command and control servers, and provide MD5s of the served

malware.

## **Spamvertised**

### **Facebook**

#### **URL+redirection**

##### **chain:**

*hxxp://goo.gl/QeshtO;*

*hxxp://goo.gl/vVbrHp;*

*hxxp://goo.gl/0oSJ7z; hxxp://goo.gl/38qlq8;*

*hxxp://goo.gl/QNQhc5 ->*

*hxxps://9dvme0lk2r0osqg3qb3rlk95z.storage.googleapis.com/q1fwum32gld35 iab9d2u4o35bjsvhjhu309.html?ref=12 ->*

*hxxp://goo.gl/wKXme1 -> hxxp://www.i-justice.org/g-o-27312-gooenn.html*

**(94.23.166.27)**

*->*

*hxxp://f3c47a0d01f3ec343f57-*

*2ba5bba9317af81ae21c42000295a455.r9.cf4.*

*-*

*rackcdn.com/24471bmbqv07595?ref=27312*

*&aff*

*\_sub=27312*

*&sub*

*\_id=27312*

*->*

*hxxp://www.eklentidunyasi.com/dl.php (176.31.2.155) or  
hxxp://www.agentofex.com/dl.php (176.227.218.99;  
www.puee.in) ->*

*hxxp://docs.google.com/uc?export=download*

*&id=0B6DFdqpSFDAISmpsTkZkT2hvN28*

*or*

*hxxps://doc-*

*0g-4o-*

*docs.googleusercontent.com/docs/securesc/ha0ro937gcu*

*c7l7deffksulhg5h7mbp1/7fbm9gn-*

*67t8t18r8etd00juf0rvmrrmh/1387836000000/1*

*6300082901287672546/\*/0BzU3dARQGry0TIMxN3F2STN0Z3  
M*

**GA Account ID:** UA-36486228-1

841

<http://goo.gl/wKXme1>

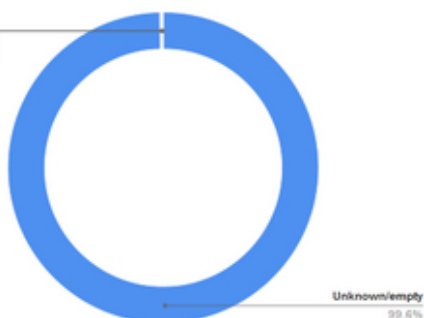
<http://www.i-justice.org/g-o-27312-gooenn.html>

Created: 2013 Dec 23

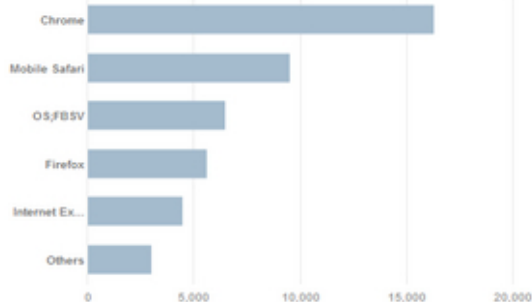


#### Referrers

Other  
0.2%  
Others  
0.2%



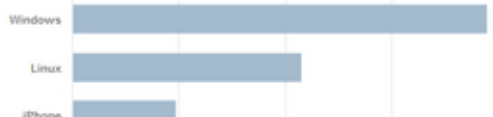
#### Browsers



#### Countries



#### Platforms



**Detection rate for the served malware: [3]MD5: 30118bec581f80de46445aef79e6cf10** - detected by 33 out of 48

antivirus scanners as Trojan-Ransom.Win32.Blocker.dbud.

Once executed, the sample phones back to:

hxxp://176.31.2.155/extFiles/control8.txt

hxxp://176.31.2.155/extFiles/NewFile0008.exe

hxxp://176.31.2.155/extFiles/version.txt



hxxp://176.31.2.155/extFiles/list.txt

hxxp://176.31.2.155/extFiles/list.txt

hxxp://176.31.2.155/extFiles/buflash.xpi

hxxp://176.31.2.155/extFiles/bune10.zip

hxxp://176.31.2.155/extFiles/private/sandbox\_status.php

hxxp://176.31.2.155/extFiles/extFiles/yok.txt

842

Now Page **985 people** total **3,457 video's** watched...



[register](#) [login](#)

[home](#) [category](#) [channel](#)

### Forget to wear pants, Selena Star sparks underwear riddle

Please install Flash Player...

15,547 watched

1 day ago

Video

share: [f](#) [t](#) [in](#) [g](#)

#### Navigator

- [home](#)
- [about us](#)
- [category](#)
- [chanelis](#)
- [faq](#)
- [contact](#)

#### Social Newtork

- [Facebook](#)
- [Twitter](#)

© 2011 - unluvideolari.info

The files were offline in time of processing of the sample.

### **Related MD5s for the same served fake Adobe Flash Player:**

MD5: 61f5af5d0067ea8d10f0764ff3c82066

MD5: 80b9ef43183abdd5b22482bc1cea7b36

MD5: 2da7cb838234eebbca3115fcafd6f513

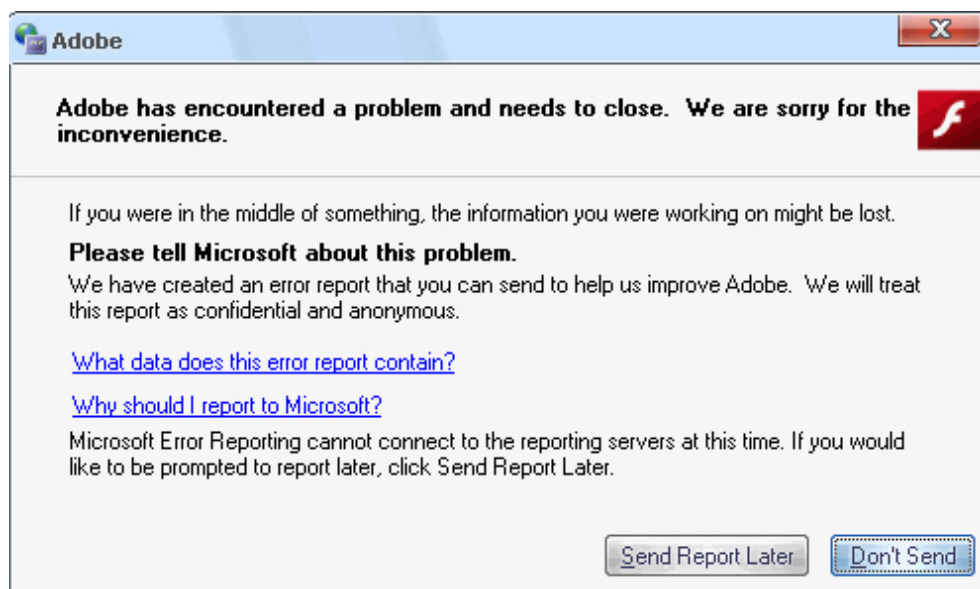
MD5: 40ae8d901102ee3951c241b394eb94e9

MD5: 30118bec581f80de46445aef79e6cf10

MD5: 2de9865032e997d59c03bfd8435f1ada

MD5: fce013bec7b3651c100b6887c0a12eee

843



**Once executed, MD5:  
fce013bec7b3651c100b6887c0a12eee phones back  
to:**

hxxp://176.227.218.99/extFiles/control17.txt

hxxp://176.227.218.99/extFiles/NewFile00017.exe

hxxp://46.163.100.240/NewFile00017.exe

hxxp://176.227.218.99/NewFile00017.exe

hxxp://176.227.218.99/extFiles/extFiles/version.txt

hxxp://176.227.218.99/extFiles/extFiles/list.txt

hxxp://176.227.218.99/extFiles/extFiles/buflash.xpi

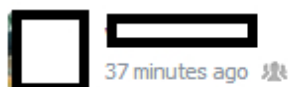
hxxp://176.227.218.99/extFiles/extFiles/bune10.zip

Files remain offline in the time of processing of the sample.

1. <http://ddanchev.blogspot.com/2013/12/continuing-facebook-whos-viewed-your.html>

2. <http://ddanchev.blogspot.com/2013/12/facebook-circulating-whos-viewed-your.html>

3. <https://www.virustotal.com/en/file/ade1707efaa1496691d5d4b12daadff893b0f0ad68b33699e5dd7dd6f8eb58/analysis/1387838333/>



My profile has been viewed today 712 times.

Top 5 Visitors:

- 1- [redacted] visits
- 2- [redacted] visits
- 3- [redacted] 0 visits
- 4- [redacted] 38 visits
- 5- [redacted] 16 visits

See who has viewed your profile HERE:

<http://GXOMZRC.tk/?74604844> — with [redacted] and 48 others.

## **Dissecting the Ongoing Febipos/Carfekab Rogue Chrome/Firefox Extensions Dropping, Facebook Circulat-**

### **ing Malicious Campaign (2014-01-09 17:21)**

And, (not surprisingly) they're back! The cybercriminal(s) behind the 1 million+ clicks strong Febipos/Carfekab rogue

Chrome/Firefox extensions dropping malicious campaign, continue utilizing the already infected 'population' for

the purpose of disseminating the newly packed/modified extensions/samples across Facebook, with yet another campaign that I'll dissect in this post.

## Catch up with previous research dissecting the previous campaigns:

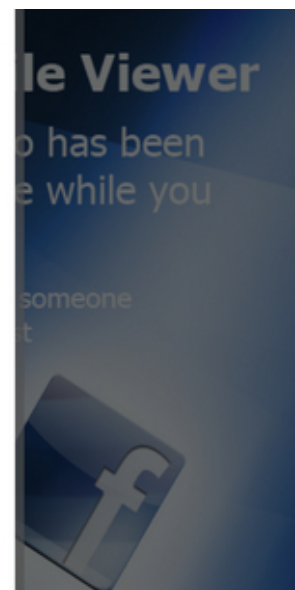
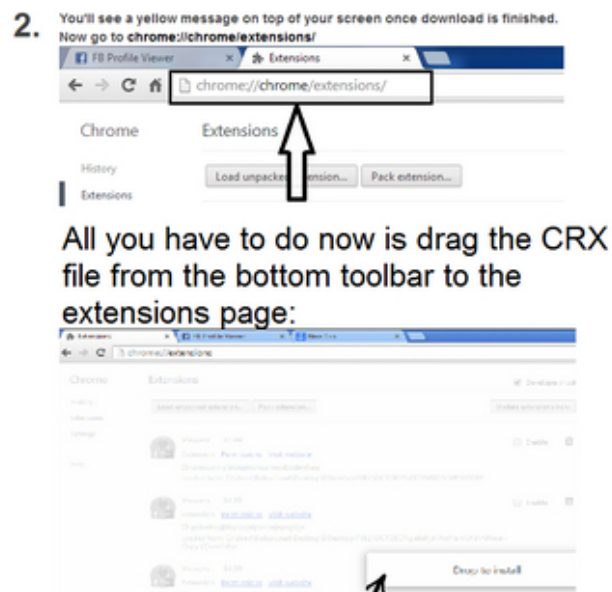
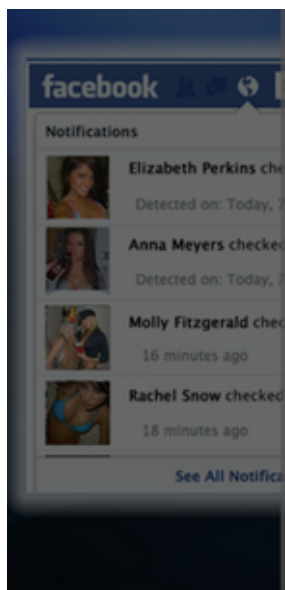
- [1] Facebook Circulating 'Who's Viewed Your Profile' Campaign Exposes 800k+ Users to CrossRider PUA/Rogue

Firefox Add-ons/Android Adware AirPush

- [2] Continuing Facebook "Who's Viewed Your Profile" Campaign Affects Another 190k+ Users, Exposes Malicious

Cybercrime Ecosystem

**Redirection chain:** *hxxp://GXOMZRC.tk/?74604844 (93.170.52.34) -> hxxp://wqeuijks.igg.biz/?asdjas2222222-222222 (88.198.132.3) -> hxxp://prostats.vf1.us/s.htm -> hxxp://vidsvines.com/d/ -> hxxp://vidsvines.com/d/firefox 845*



->

*hxxp://vidsvines.com/d/ch/ ->*

*hxxp://vidsvines.com/d/ch/profile2.html (192.157.201.42)*

**First GA Account ID:** UA-23441223-3

**Second GA Account ID:** UA-25941572-1

**Actual malicious content hosting locations  
(legitimate infrastructure again):**

*hxxps://docs.google.com/uc?authuser=0 &id=0BziH-  
mKCcuQwqVFgyZzFzR1o3YTQ &export=download*

*hxxps://dl.dropboxusercontent.com/s/tj9n05qhjvnkg4s/whovi  
ewsfam.xp i*

**Detection rates for the served rogue Chrome/Firefox  
extensions:**

**[3]MD5: 0ee44443c73bd9b072c7f1dbb6b7b591**

**[4]MD5: c4953f63ab46c796e23388f9c1cfa273**

**[5]MD5: 5bcec283594e863f5dd238e2d22446c7**



## Who Viewed Your Profile

More ways to experience Facebook

### Introducing the new "Who Viewed Your Profile" feature on facebook!

Ever wanted to see how views your profile?  
on Facebook? Now you can!  
Let yourself do it already!  
It's Just an Extension to install.

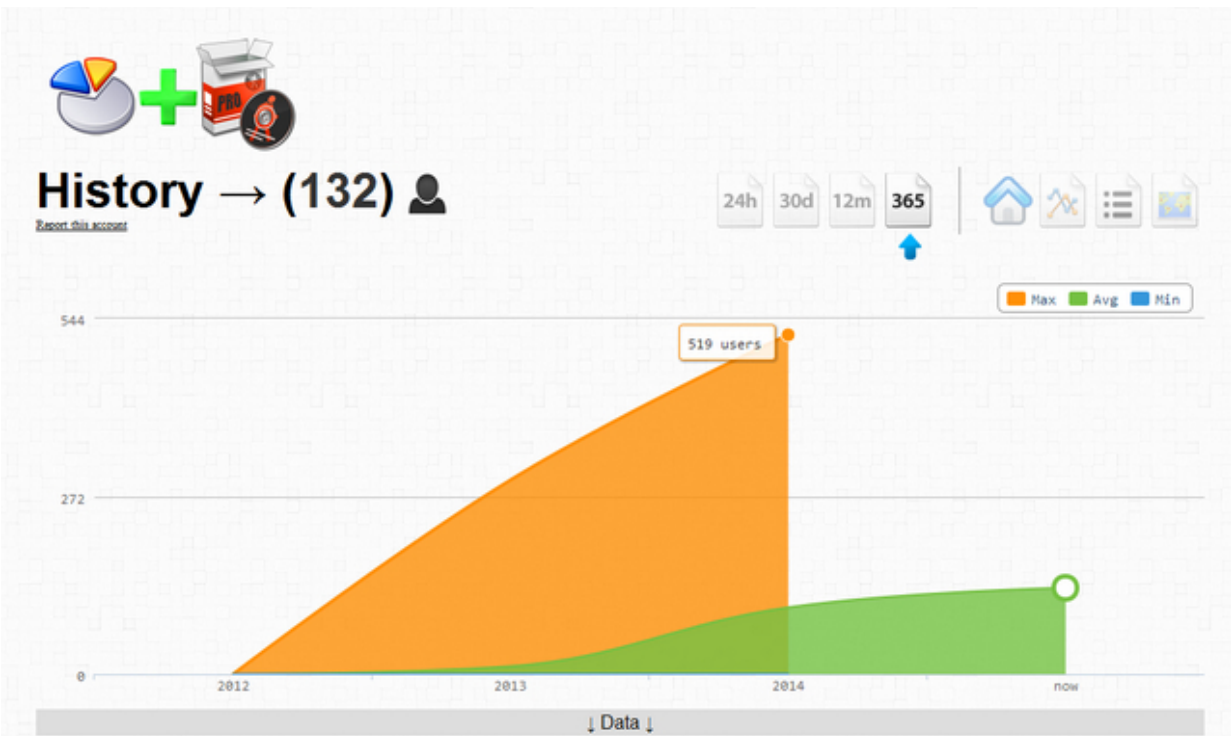


INSTALL

Once executed, [6]**MD5: 5bcec283594e863f5dd238e2d22446c7** drops **MD5: deb483270b9ed5da7fcf1d01a6fde8a7**

and **MD5: 90b77a477d815c771559d08ea80cc0c8** it then phones back to 212.117.32.20.

847



**Related malicious MD5s known to have phoned back to the same IP:**

MD5: 33408f35623dc5bb4a3bde09fa45f86b

MD5: 56a54a700ae5700c3cd3da9c2ad226cf

MD5: f86812305039156b1da8fc29bdddebb7

MD5: ede8f20d78a81c7da76ad7def37ebbdd

***This post has been reproduced from [7]Dancho Danchev's blog . Follow him [8]on Twitter.***

1. <http://ddanchev.blogspot.com/2013/12/facebook-circulating-whos-viewed-your.html>
2. <http://ddanchev.blogspot.com/2013/12/facebook-circulating-whos-viewed-your.html>



3.

<https://www.virustotal.com/en/file/ae0ac523f752b320a103befeacfc960e6f86b01343d7598f48664afcb4cedd71/analysis/1389277417/>

4.

<https://www.virustotal.com/en/file/dd46cd6ec5b139f55a9ddec75fed261568c06abf1883cf28dc1f5a3491c3e0c1/analysis/1389277591/>

5.

<https://www.virustotal.com/en/file/7737cf0c74e5e84f543a379ff9e42ac372f78ff0e8eb4c847a7bc4d07f8b1368/analysis/1389277807/>

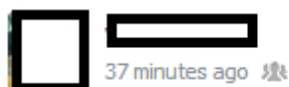
6.

<https://www.virustotal.com/en/file/7737cf0c74e5e84f543a379ff9e42ac372f78ff0e8eb4c847a7bc4d07f8b1368/analysis/1389277807/>

7. <http://ddanchev.blogspot.com/>

8. <http://twitter.com/danchodanchev>

848



37 minutes ago

My profile has been viewed today 712 times.

Top 5 Visitors:

- 1- [redacted] 1 visits
- 2- [redacted] 1 visits
- 3- [redacted] 10 visits
- 4- [redacted] 38 visits
- 5- [redacted] 16 visits

See who has viewed your profile HERE:

<http://GXOMZRC.tk/?74604844> — with [redacted] and 48 others.

## **Dissecting the Ongoing Febipos/Carfekab Rogue Chrome/Firefox Extensions Dropping, Facebook Circulat-**

### **ing Malicious Campaign (2014-01-09 17:21)**

And, (not surprisingly) they're back! The cybercriminal(s) behind the 1 million+ clicks strong Febipos/Carfekab rogue

Chrome/Firefox extensions dropping malicious campaign, continue utilizing the already infected 'population' for

the purpose of disseminating the newly packed/modified extensions/samples across Facebook, with yet another campaign that I'll dissect in this post.

## **Catch up with previous research dissecting the previous campaigns:**

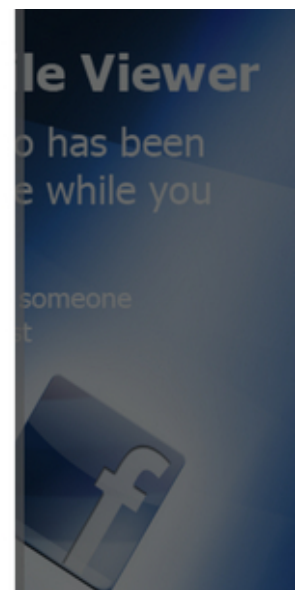
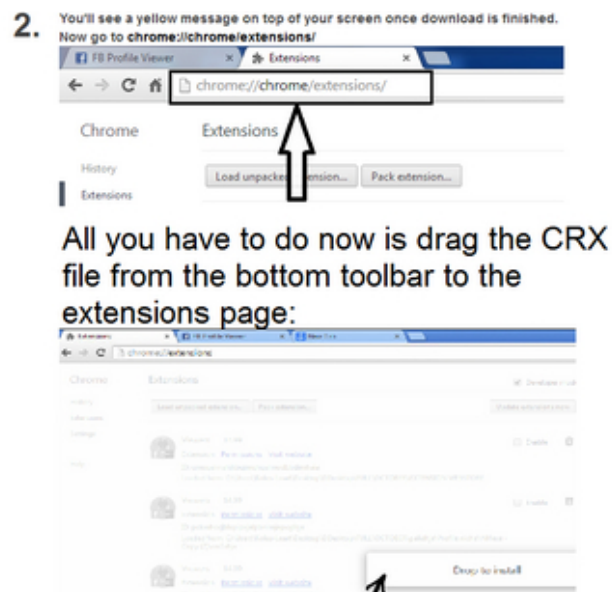
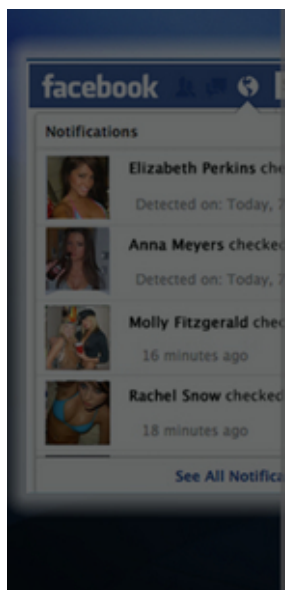
- [1]Facebook Circulating 'Who's Viewed Your Profile' Campaign Exposes 800k+ Users to CrossRider PUA/Rogue

Firefox Add-ons/Android Adware AirPush

- [2]Continuing Facebook "Who's Viewed Your Profile" Campaign Affects Another 190k+ Users, Exposes Malicious

Cybercrime Ecosystem

**Redirection chain:** *hxxp://GXOMZRC.tk/?74604844 (93.170.52.34) -> hxxp://wqeuijks.igg.biz/?asdj22222222-222222 (88.198.132.3) -> hxxp://prostats.vf1.us/s.htm -> hxxp://vidsvines.com/d/ -> hxxp://vidsvines.com/d/firefox 849*



->

*hxxp://vidsvines.com/d/ch/ ->*

*hxxp://vidsvines.com/d/ch/profile2.html (192.157.201.42)*

**First GA Account ID:** UA-23441223-3

**Second GA Account ID:** UA-25941572-1

**Actual malicious content hosting locations  
(legitimate infrastructure again):**

*hxxps://docs.google.com/uc?authuser=0 &id=0BziH-  
mKCcuQwqVFgyZzFzR1o3YTQ &export=download*

*hxxps://dl.dropboxusercontent.com/s/tj9n05qhjvnkg4s/whovi  
ewsfam.xp i*

**Detection rates for the served rogue Chrome/Firefox  
extensions:**

**[3]MD5: 0ee44443c73bd9b072c7f1dbb6b7b591**

**[4]MD5: c4953f63ab46c796e23388f9c1cfa273**

**[5]MD5: 5bcec283594e863f5dd238e2d22446c7**

850



## Who Viewed Your Profile

More ways to experience Facebook

### Introducing the new "Who Viewed Your Profile" feature on facebook!

Ever wanted to see how views your profile?  
on Facebook? Now you can!  
Let yourself do it already!  
It's Just an Extension to install.



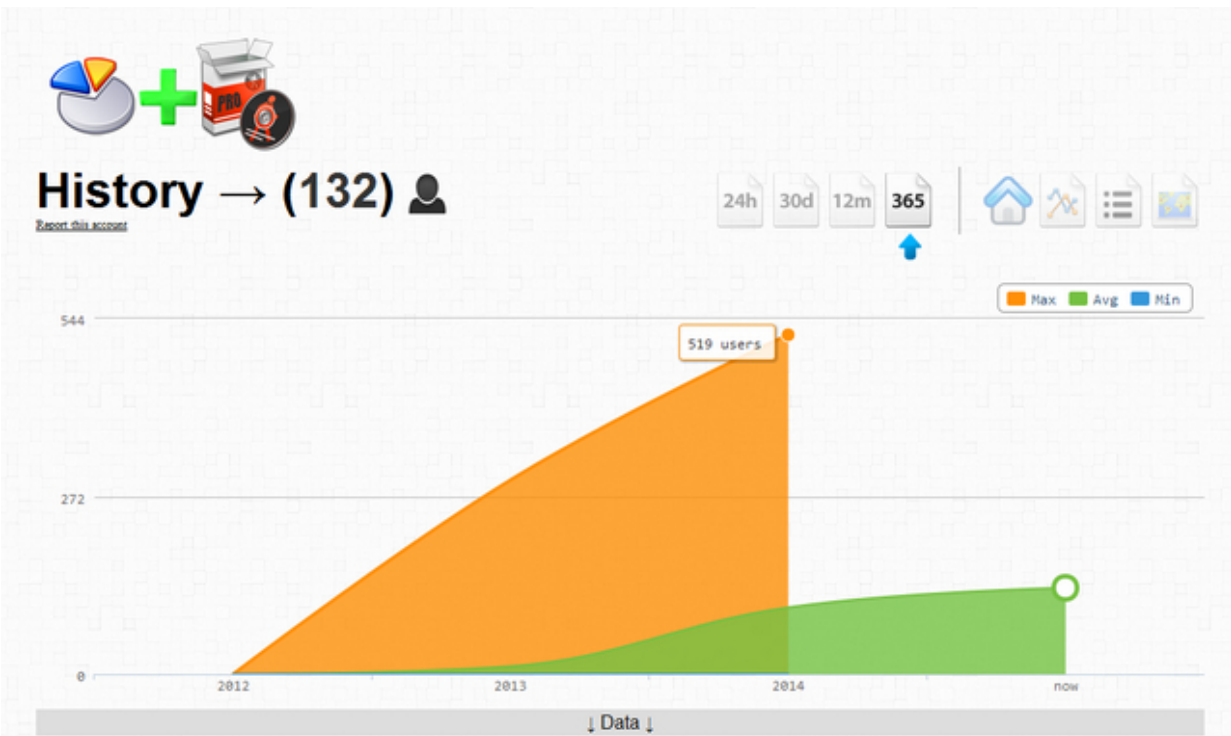
INSTALL

Once executed, [6]**MD5:**

**5bcec283594e863f5dd238e2d22446c7** drops **MD5:**  
**deb483270b9ed5da7fcf1d01a6fde8a7**

and **MD5: 90b77a477d815c771559d08ea80cc0c8** it  
then phones back to 212.117.32.20.

851



## **Related malicious MD5s known to have phoned back to the same IP:**

MD5: 33408f35623dc5bb4a3bde09fa45f86b

MD5: 56a54a700ae5700c3cd3da9c2ad226cf

MD5: f86812305039156b1da8fc29bdddebb7

MD5: ede8f20d78a81c7da76ad7def37ebbdd

**Updates will be posted as soon as new developments take place.**

1. <http://ddanchev.blogspot.com/2013/12/facebook-circulating-whos-viewed-your.html>
2. <http://ddanchev.blogspot.com/2013/12/facebook-circulating-whos-viewed-your.html>

3.

<https://www.virustotal.com/en/file/ae0ac523f752b320a103befeacfc960e6f86b01343d7598f48664afcb4cedd71/analysis/1389277417/>

[is/1389277417/](https://www.virustotal.com/en/file/ae0ac523f752b320a103befeacfc960e6f86b01343d7598f48664afcb4cedd71/analysis/1389277417/)

4.

<https://www.virustotal.com/en/file/dd46cd6ec5b139f55a9dde75fed261568c06abf1883cf28dc1f5a3491c3e0c1/analysis/1389277591/>

[is/1389277591/](https://www.virustotal.com/en/file/dd46cd6ec5b139f55a9dde75fed261568c06abf1883cf28dc1f5a3491c3e0c1/analysis/1389277591/)

5.

<https://www.virustotal.com/en/file/7737cf0c74e5e84f543a379ff9e42ac372f78ff0e8eb4c847a7bc4d07f8b1368/analysis/1389277807/>

[is/1389277807/](https://www.virustotal.com/en/file/7737cf0c74e5e84f543a379ff9e42ac372f78ff0e8eb4c847a7bc4d07f8b1368/analysis/1389277807/)

6.

<https://www.virustotal.com/en/file/7737cf0c74e5e84f543a379ff9e42ac372f78ff0e8eb4c847a7bc4d07f8b1368/analysis/1389277807/>

[is/1389277807/](https://www.virustotal.com/en/file/7737cf0c74e5e84f543a379ff9e42ac372f78ff0e8eb4c847a7bc4d07f8b1368/analysis/1389277807/)

852



3 hours ago

Reyting ugruna her gun neler goruyoruz vallahi yazik!8 lygh18gds4i Valla bunlarda kisilik falan kalmamis kardesimX Bunlar da hakli hic bir yetenegi olmayan insanlar sonucta bunlar!Y zslqsemi — with [redacted] and 18 others.



[redacted] Videoyu izledim. Rezillik!!

insmi.com

Yari ciplak bir sekilde programa katilmak? Arkadaslar izleyin yorumunuzu bekliyorum!

Like • Comment • Share

**Facebook Spreading,**

**Amazon AWS/Cloudflare/Google Docs Hosted Campaign,**

**Serves P2P-**

**Worm.Win32.Palevo (2014-01-16 21:27)**

A currently circulating across Facebook, multi-layered monetization tactics utilizing, Turkish users targeting, malicious

campaign, is attempting to trick users into thinking that they need to install a fake Adobe Flash Player, displayed

on a fake YouTube Video page, ultimately serving P2P-Worm.Win32.Palevo on the hosts of the socially engineered

(international) users.

Let's dissect the campaign, expose its infrastructure in terms of shortened URLs, redirectors, affiliate network

IDs, landing pages, pseudo-random Facebook content generation phone back URLs, legitimate infrastructure hosted

content, and provide MD5s for the served malicious content.

**Sample**

**redirection**

**chain:**

*hxxp://m3mi.com/10469*



->

*hxxp://facebookikiziniz.com/yon.html?MYt-DmZp4xjbUP9A0OHLj*

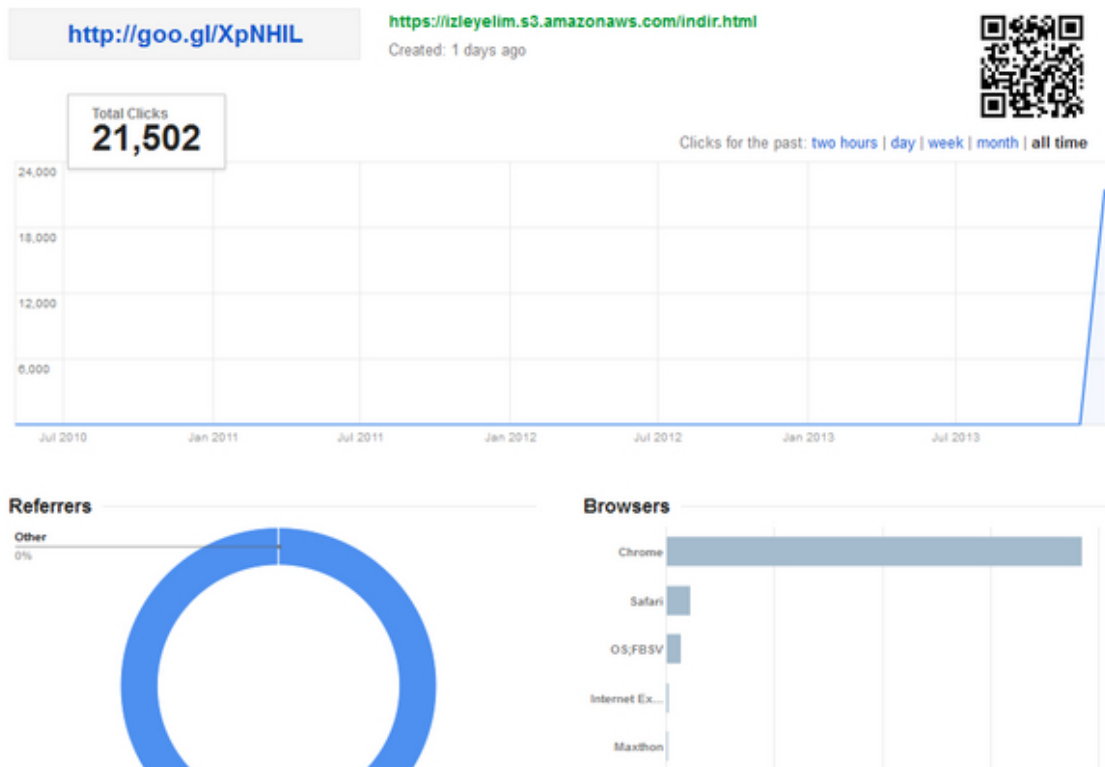
->

*hxxp://facebookikiziniz.com/yon.html?MYtDmZp4xjbUP9A0OHLj*

->

*hxxp://facebookikiziniz.com/yon.html?MYtDmZp4xjbUP9A0OHLj*

853



**Internal campaign redirection structure+associated affiliate network IDs+landing URLs:**

*hxxp://mobiltrafik.s3.amazonaws.com/mobil.html*

*hxxp://mobiltrafik.s3.amazonaws.com/yurtdisi-anroid.html ->*

*hxxp://ad.adrttt.com/aff\_c?offer\_id=1743 &aff\_id=3236*

*&source=yurtdisi ->*

*hxxp://ads.glispa.com/sw/49399/CD353/102*

*3a788c68361b710b87b8ed4851a ->*

*hxxps://play.google.com/store/apps/details?*

*id=com.mobogenie.marketstl*

*hxxp://mobiltrafik.s3.amazonaws.com/yurtdisi-ios.html*

*->*

*hxxp://ad.rdrttt.com/aff*

*\_c?offer*

*\_id=302*

*&aff*

*\_id=1014*

*->*

*hxxp://www.freehardcorepassport.com/?t=116216,1,96,0*

*&x=pornfr*

*\_tracker=9208K0m00B0193lbJl3yk01BNW00005m*

*hxxp://mobiltrafik.s3.amazonaws.com/yurtdisiweb.html ->*

*hxxp://ad.rdrttt.com/aff\_c?offer\_id=302 &aff\_id=1014*

*-> hxxp://ads.polluxnetwork.com/hosted/w2m.php?*

*tid=1023e4f08cae470c2f74aa 3d1e2d17 &oid=6200*

*&aid=758*

-> [hxxp://m.pornfr.3013.idhad.com/xtrem/index.wiml](http://m.pornfr.3013.idhad.com/xtrem/index.wiml)

[hxxp://mobiltrafik.s3.amazonaws.com/androidwifi.html](http://mobiltrafik.s3.amazonaws.com/androidwifi.html) ->

[hxxp://ad.adrttt.com/aff\\_c?offer\\_id=1743 &aff\\_id=3236](http://ad.adrttt.com/aff_c?offer_id=1743&aff_id=3236)

[&source=yurtici](#) ->

[hxxp://ads.glispa.com/sw/49399/CD353/102](http://ads.glispa.com/sw/49399/CD353/102)

[3a788c68361b710b87b8ed4851a](#)

[hxxp://mobiltrafik.s3.amazonaws.com/iphonewifi.html](http://mobiltrafik.s3.amazonaws.com/iphonewifi.html) ->

[hxxp://ad.adrttt.com/aff\\_c?offer\\_id=1705 &aff\\_id=3236](http://ad.adrttt.com/aff_c?offer_id=1705&aff_id=3236)

-> [hxxps://itunes.apple.com/tr/app/id451786983?mt=8](http://itunes.apple.com/tr/app/id451786983?mt=8)

[hxxp://mobiltrafik.s3.amazonaws.com/turkcell.html](http://mobiltrafik.s3.amazonaws.com/turkcell.html) ->

[hxxp://goo.gl/GBKArV](http://goo.gl/GBKArV)

[hxxp://mobiltrafik.s3.amazonaws.com/vodafone.html](http://mobiltrafik.s3.amazonaws.com/vodafone.html) ->

[hxxp://ad.adrttt.com/aff\\_c?offer\\_id=1785 &aff\\_id=3236](http://ad.adrttt.com/aff_c?offer_id=1785&aff_id=3236)

-> [hxxp://c.mobpartner.mobi/?s=1007465 &a=3578](http://c.mobpartner.mobi/?s=1007465&a=3578)

[&tid1=102afc4360ecadbed491b5c08f7395](#)

[hxxp://mobiltrafik.s3.amazonaws.com/avea.html](http://mobiltrafik.s3.amazonaws.com/avea.html) ->

[hxxp://ad.juksr.com/aff\\_c?offer\\_id=709 &aff\\_id=3236](http://ad.juksr.com/aff_c?offer_id=709&aff_id=3236)

->

[hxxp://wap.chatwalk.com/landings/?name=yilbasi2](http://wap.chatwalk.com/landings/?name=yilbasi2)

[&affid=reklamaction](#)

[&utm](#)

[\\_campaign=3236](#)

[&clk=1025fa187aca81ce57edf8adca7a9c](#)

*hxxp://mobiltrafik.s3.amazonaws.com/trweb.html ->*  
*hxxp://ad.adrttt.com/aff\_c?offer\_id=1689 &aff\_id=3236*

*&source=yurticidefault ->*  
*hxxps://www.matchandtalk.com/splashmobile/10?sid=12*  
*&bid=663*

*hxxp://s3.amazonaws.com/Yonver/tarayici.html ->*  
*hxxp://ad.adrttt.com/aff\_c?offer\_id=1091 &aff\_id=3236*

*&source=tarayicidan ->*  
*hxxps://www.matchandtalk.com/splash/12?sid=12*  
*&bid=651 &cid=29*

*hxxp://izleyelim.s3.amazonaws.com/unlu.html*

*->*

*hxxp://goo.gl/XpNHIL*

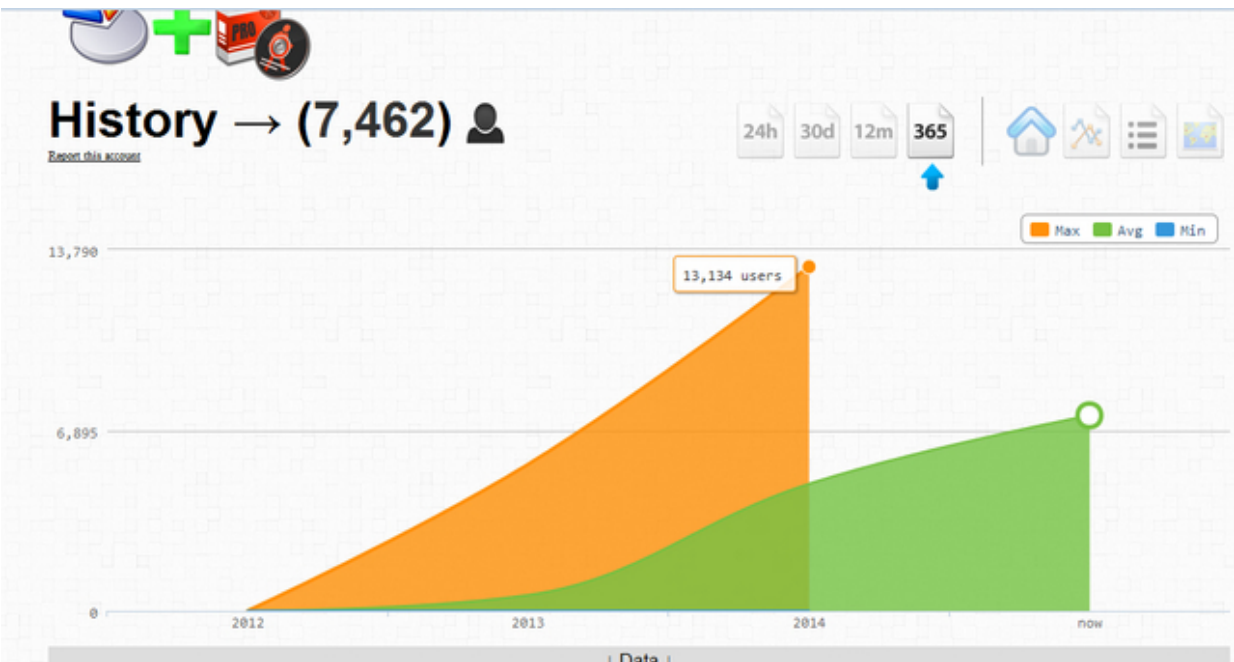
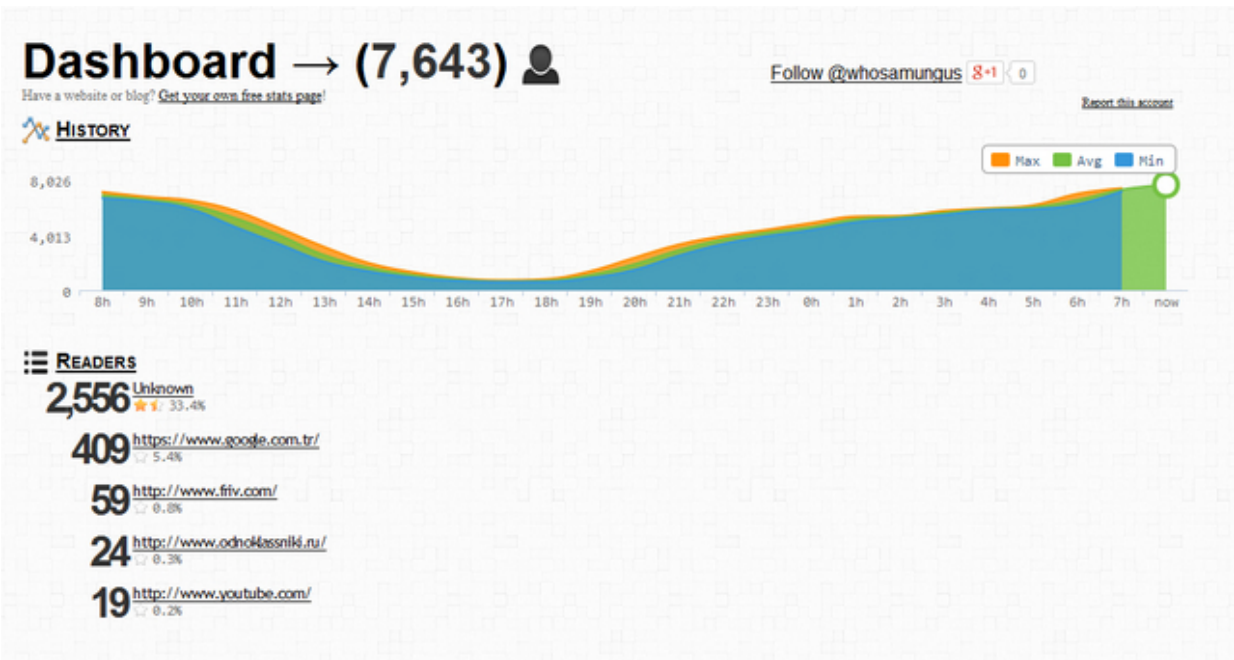
*(21,512*

*clicks)*

*->*

*hxxps://izleyelim.s3.amazonaws.com/indir.html*

*854*



<https://s3.amazonaws.com/facebookAds/ortaryon.html>

->

<https://www.matchandtalk.com/splash/12?sid=12>

[&bid=651 &cid=29](#)

## Malicious/fraudulent domain name reconnaissance:

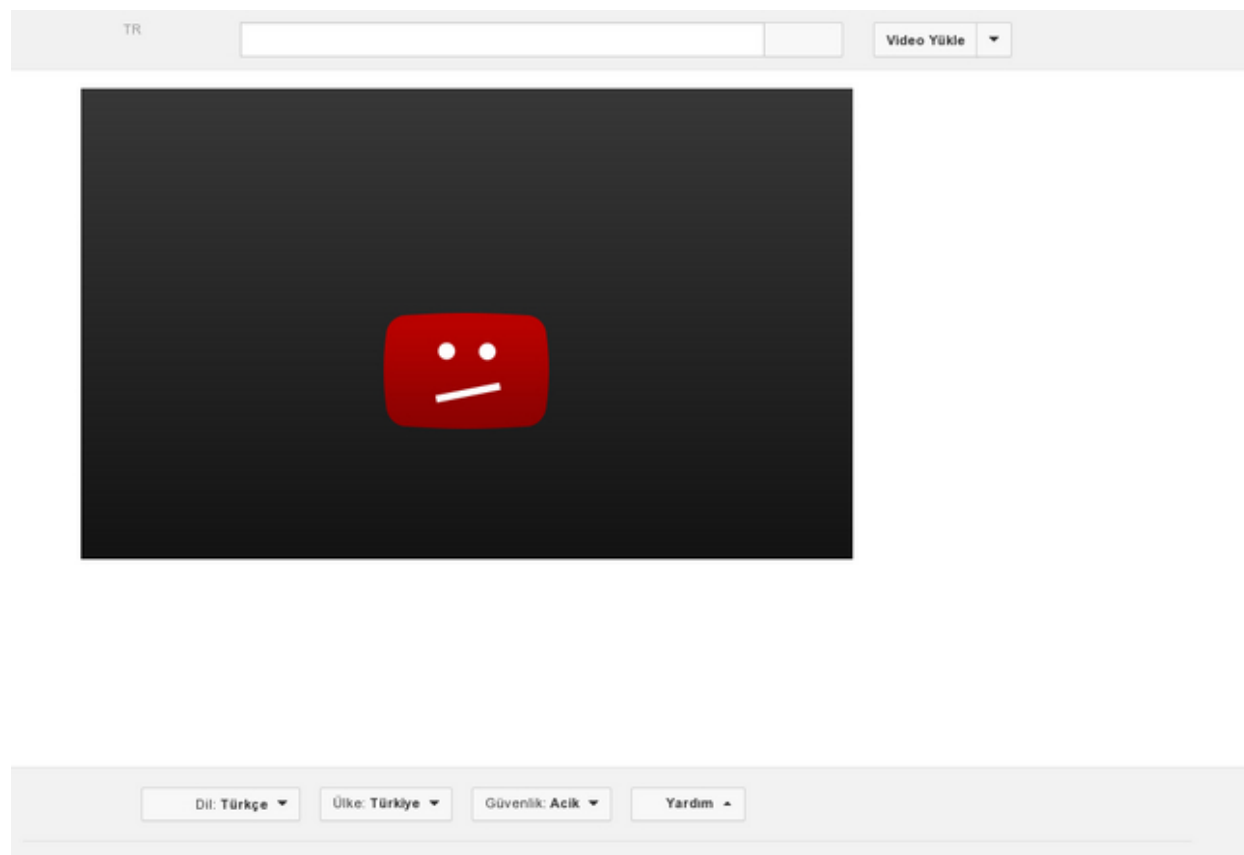
facebookikiziniz.com - 108.162.195.103; 108.162.194.103

ttcomcdn.com - 162.159.241.195; 162.159.242.195 - Email: masallahkilic@hotmail.com

amentosx.com - 141.101.116.113; 141.101.117.113

ad.adrttt.com - 54.236.194.194

855



The campaign is also mobile device/PC-aware, and is therefore automatically redirecting users to a variety of different

locations/affiliate networks. Case in point, the redirection to Google Play's Mobogenie Market App (Windows appli-

cation detected as Adware.NextLive.2 [1]**MD5: 9dd785436752a6126025b549be644e76**), and the iOS compatible SK

planet's TicToc app.

Now comes the malicious twist, in the form of Fake Adobe Flash Player, that socially engineered users would

have to install, in order to view the non-existent YouTube video content.

### **Actual Fake Adobe Flash Player hosting locations within Google Docs:**

*hxxps://docs.google.com//uc?authuser=0 &id=0B9oVyH\_w8BCFcWZIRGY0V1lxNVU*

*hxxps://docs.google.com//uc?authuser=0 &id=0B9oVyH\_w8BCFQVBsdVVOekYyNGs*

*hxxps://docs.google.com//uc?authuser=0 &id=0B9oVyH\_w8BCFaEN2TnE4M0sxWHM*

*hxxps://docs.google.com//uc?authuser=0 &id=0B9oVyH\_w8BCFVXRnbkYtNG5wVDA*

*hxxps://docs.google.com//uc?authuser=0 &id=0B9oVyH\_w8BCFR2NnRXFRUmtNTTQ*

*hxxps://docs.google.com//uc?authuser=0 &id=0B9oVyH\_w8BCFOWFGZnlxMkZWcUE*

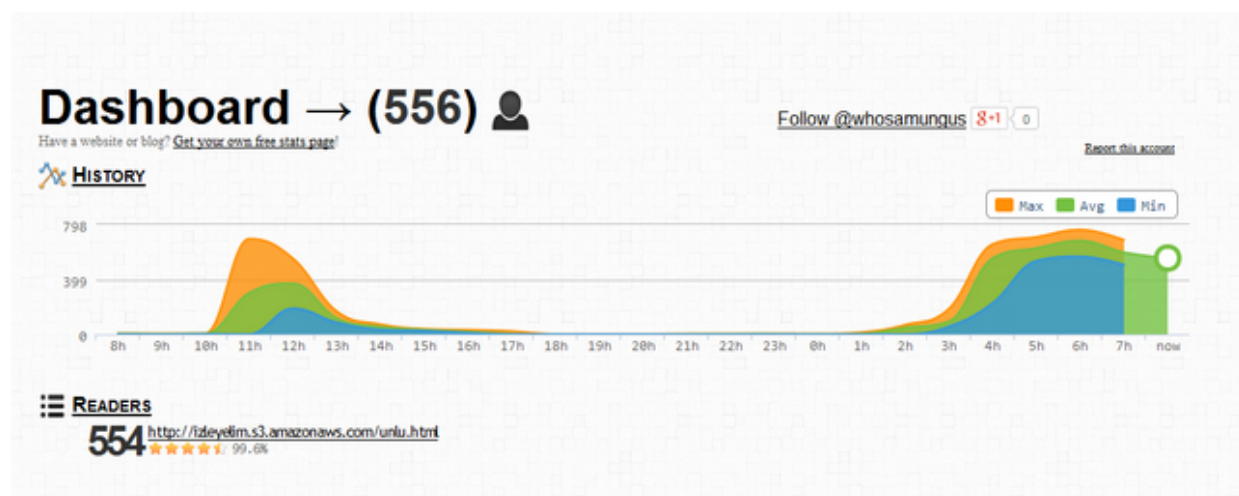
*hxxps://docs.google.com//uc?authuser=0 &id=0B9oVyH\_w8BCFcWZZbTljMkJWZ3c*

[hxxps://docs.google.com//uc?authuser=0 &id=0B9oVyH\\_w8BCFYkpEdXI4ZGVaaUE](https://docs.google.com//uc?authuser=0&id=0B9oVyH_w8BCFYkpEdXI4ZGVaaUE)

[hxxps://docs.google.com//uc?authuser=0 &id=0B9oVyH\\_w8BCFMUxzY0dQTTJMV00](https://docs.google.com//uc?authuser=0&id=0B9oVyH_w8BCFMUxzY0dQTTJMV00)

[hxxps://docs.google.com//uc?authuser=0 &id=0B9oVyH\\_w8BCFNmROShMSGdCYUU](https://docs.google.com//uc?authuser=0&id=0B9oVyH_w8BCFNmROShMSGdCYUU)

856



[hxxps://docs.google.com//uc?authuser=0 &id=0B9oVyH\\_w8BCFb0RoZVltMmsyRFU](https://docs.google.com//uc?authuser=0&id=0B9oVyH_w8BCFb0RoZVltMmsyRFU)

[hxxps://docs.google.com//uc?authuser=0 &id=0B9oVyH\\_w8BCFb2k2MFN4QTY1ZUE](https://docs.google.com//uc?authuser=0&id=0B9oVyH_w8BCFb2k2MFN4QTY1ZUE)

[hxxps://docs.google.com//uc?authuser=0 &id=0B9oVyH\\_w8BCFb1AzZXI4emlGR00](https://docs.google.com//uc?authuser=0&id=0B9oVyH_w8BCFb1AzZXI4emlGR00)

[hxxps://docs.google.com//uc?authuser=0 &id=0B9oVyH\\_w8BCFSDZBRDJ4QjVqdkU](https://docs.google.com//uc?authuser=0&id=0B9oVyH_w8BCFSDZBRDJ4QjVqdkU)

[hxxps://docs.google.com//uc?authuser=0 &id=0B9oVyH\\_w8BCFUXgtZ1VQVU9OdVU](https://docs.google.com//uc?authuser=0&id=0B9oVyH_w8BCFUXgtZ1VQVU9OdVU)



*hxxps://docs.google.com//uc?authuser=0 &id=0B9oVyH  
\_w8BCFUll6c0Y0MWxLZW8*

*hxxps://docs.google.com//uc?authuser=0 &id=0B9oVyH  
\_w8BCFSW55S3R0SWcxdDQ*

*hxxps://docs.google.com//uc?authuser=0 &id=0B9oVyH  
\_w8BCFMWtxaGJTMnpMVDA*

*hxxps://docs.google.com//uc?authuser=0 &id=0B9oVyH  
\_w8BCFSk9yUW5ldDVKaUU*

*hxxps://docs.google.com//uc?authuser=0 &id=0B9oVyH  
\_w8BCFN3pTXzcxcdIObkU*

*hxxps://docs.google.com//uc?authuser=0 &id=0B9oVyH  
\_w8BCFQ0p3dV9qcC1uOFU*

*hxxps://docs.google.com//uc?authuser=0 &id=0B9oVyH  
\_w8BCFOFZRcDZwa0ZfcVk*

*hxxps://docs.google.com//uc?authuser=0 &id=0B9oVyH  
\_w8BCFNkoyNktzQ2dJVIE*

*hxxps://docs.google.com//uc?authuser=0 &id=0B9oVyH  
\_w8BCFS2xjdTE4Nk04QnM*

### **Detection rate for the fake Adobe Flash Player:**

**[2]MD5:**

**5bf26bd488503a4b2b74c7393d4136e3** - detected by 3  
out of 47 antivirus scanners as P2P-

Worm.Win32.Palevo.hexb; PE:Trojan.VBInject!1.6546

**Once executed, the sample also drops:**

**Once executed, the sample phones back to:**  
akillitefonburada.com (108.162.196.162).

[illegible]

## Sample

**pseudo-random**

**bogus**

**Facebook**

**content**

**generation**

**takes**

**place**

**through:**

hxxp://www.amentosx.com/ext/r.php

->

hxxps://s3.amazonaws.com/facebookAds/arkadaj.html

->

hxxp://ttcomcdn.com/tw.php

***This post has been reproduced from [4]Dancho Danchev's blog . Follow him [5]on Twitter.***

1.

<https://www.virustotal.com/en/file/bc9c9cb2a1219b87cdb9e356b72f2e64c1ac2e9250302e72b426ad51dcc6818f/analysis/1389893847/>

2.

<https://www.virustotal.com/en/file/9c92331776087bc46053dcf388394acdb6faace813153f6f1cd9a9be1ffad0c5/analysis/>

[is/](#)

3.

<https://www.virustotal.com/en/file/d792c1ee1f944940f1fabda43392231021596dd546a40eeb0ca407535fbc7820/analysis/>

[is/](#)

4. <http://ddanchev.blogspot.com/>

5. <http://twitter.com/danchodanchev>

858

Şuan sitedeki 985 kişi toplam 3,457 video'nun keyfini çıkarıyor.. Sizde onlardan birisi olun!

- [kayıt ol](#)
- [giriş yap](#)
- [anasayfa](#)
- [kategoriler](#)
- [kanallar](#)

#### # Recep İvedik 4 ( Full İzle - HD Ücretsiz )

Please install Flash Player...

1 gün önce eklendi

15,547 kez izlendi

Paylaş:

[Video](#)

© 2011 - unluvideolari.info

- Hızlı Menü
- [anasayfa](#)
- [hakkımızda](#)
- [kategoriler](#)
- [kanallar](#)
- [sss](#)
- [iletişim](#)
- Sosyal Ağlar
- [Facebook Sayfamız](#)
- [Twitter'dan Takip Edin!](#)
- [Videolara Abone Olun!](#)
- [İletişime Geçin!](#)

**Facebook Spreading,**

## **Amazon AWS/Cloudflare/Google Docs Hosted Campaign,**

### **Serves P2P-**

#### **Worm.Win32.Palevo (2014-01-16 21:27)**

I've recently spotted a malicious, cybercrime-friendly SWF iframe/redirector injecting service, that also exposes a

long-run Win32.Nixofro serving malicious infrastructure, currently utilized for the purpose of operating a rogue social

media service provider, that's targeting Turkish Facebook users through the ubiquitous social engineering vector, for

such type of campaigns, namely, the fake Adobe Flash player.

Let's profile the service, discuss its relevance in the broader context of the threat landscape, provide action-

able/historical threat intelligence on the malicious infrastructure, the rogue domains involved in it, the malicious

MD5s served by the cybercriminals behind it, and directly link it to a [1]**previously profiled Facebook spreading**

#### **P2P-Worm.Win32.Palevo serving campaign.**

The managed SWF iframe/redirector service, is a great example of a cybercrime-as-a-service type of underground

market proposition, empowering, both, sophisticated and novice cybercriminals with the necessary ([2]**malvertising**)

'know-how', in an efficient manner, directly intersecting with the commercial availability of [3]**sophisticated mass**

**Web site/[4]Web server** malicious script embedding platforms.

The managed SWF iframe/redirector injecting service is currently responding to 108.162.197.62 and 108.162.196.62

859

|                 | Обычный | Оптовый | VIP персона |
|-----------------|---------|---------|-------------|
| Неделя (7 дней) | 5       | 1       | 0.5         |
| Месяц (30 дней) | 10      | 2       | 1           |
| Год (365 дней)  | 15      | 5       | 2           |

Known to have responded to the same IPs (108.162.197.62; 108.162.196.62) is also a key part of the malicious

infrastructure that I'll expose in this post, namely **hizliservis.pw** - Email: furkan@cod.com.

**Known to have phoned back to the same IP (108.162.197.62) are also the following malicious MD5s:**

MD5: 432efe0fa88d2a9e191cb95fa88e7b36

MD5: 720ecb1cf4f28663f4ab25eedf620341

MD5: 02691863e9dfb9e69b68f5fca932e729

MD5: 69ed70a82cb35a454c60c501025415aa

MD5: cc586a176668ceef14891b15e1b412ab

MD5: 74291941bddcec131c8c6d531fcb1886

MD5: 7c27d9ff25fc40119480e4fe2c7ca987

MD5: 72c030db7163a7a7bf2871a449d4ea3c

MD5: 432efe0fa88d2a9e191cb95fa88e7b36

**Known to have phoned to the same IP  
(108.162.196.62) are also the following malicious  
MD5s:**

MD5: eda3f015204e9565c779e0725915864f

MD5: effcfe91beaf7a3ed2f4ac79525c5fc5

MD5: 14acd831691173ced830f4b51a93e1ca

MD5: 7f93b0c611f7020d28f7a545847b51e0

MD5: bcfce3a9bf2c87dab806623154d49f10

MD5: 4c90a89396d4109d8e4e2491c5da4846

MD5: 289c4f925fdec861c7f765a65b7270af

**Sample redirection chain leading to the fake Adobe  
Flash Player:**

*hxxp://hizliservis.pw/unlu.htm*

->

*hxxp://hizliservis.pw/indir.php*

->

*hxxp://unluvideolari.info*

->

*hxxp://videotr.in/player.swf*

->

*hxxp://izleyelim.s3.amazonaws.com/movie.mp4*

*&skin=newtubedark/NewTubeDark.xml &streamer=lighttpd  
&image=hqdefault.jpg*

### **Domain name reconnaissance:**

hizliservis.pw - Email: furkan@cod.com

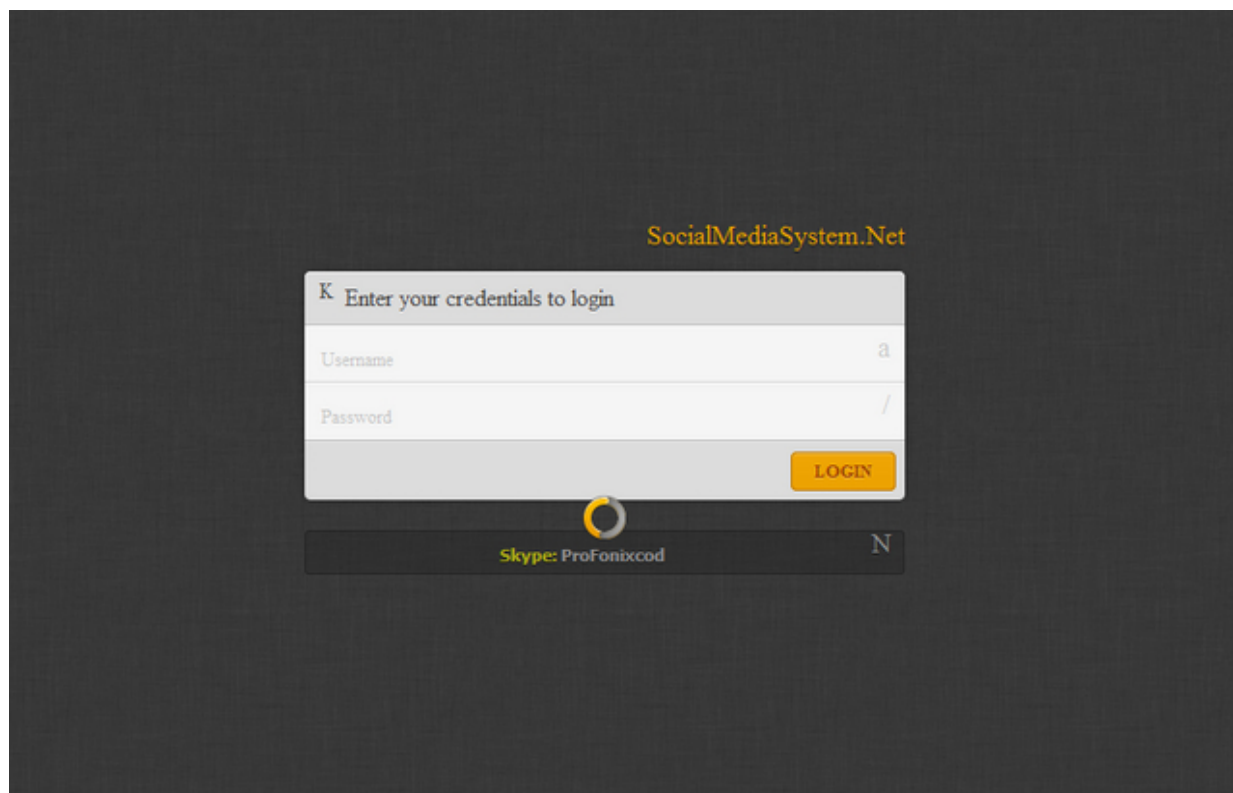
videotr.in - Email: tiiknet@yandex.com; snack@log-z.com

izleyelim.s3.amazonaws.com - 176.32.97.249

Within **hizliservis.pw**, we can easily spot yet another part of the same malicious/fraudulent infrastructure,

namely, the rogue social media distribution platform's login interface.

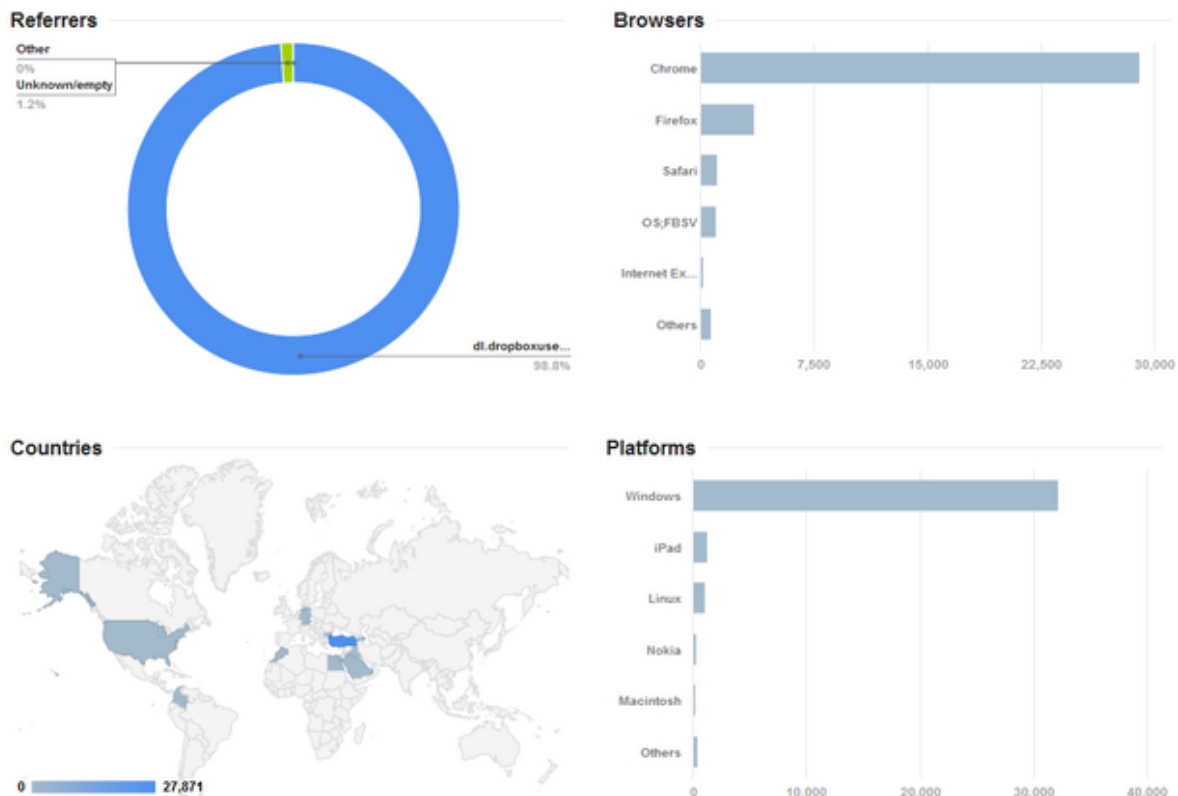




**Sample redirection chain leading to a currently active fake Adobe Flash Player (Win32.Nixofro):**

hxxp://socialmediasystem.net/down.php ->  
hxxps://profonixback31.googlecode.com/svn/FlashPlayer  
\_Guncelle.exe

861



### Detection rate for the fake Adobe Flash Player:

[5]**MD5: 28c3c503d398914bdd2c2b3fdc1f9ea4** - detected by 36 out of 50 antivirus scanners as Win32.Nixofro

Once executed, the sample phones back to **profonixuser.net** (141.101.117.218)

**Known to have responded to the same IP (141.101.117.218) are also the following malicious MD5s:**

MD5: 53360155012d8e5c648aca277cbde587

MD5: a66a1c42cc6fb775254cf32c8db7ad5b

MD5: a051fd83fc8577b00d8d925581af1a3b

MD5: f47784817a8a04284af4b602c7719cb7

MD5: 2e5c75318275844ce0ff7028908e8fb4

MD5: 90205a9740df5825ce80229ca105b9e8

**Domain name reconnaissance for the rogue social media distribution platform:**

socialmediasystem.Net (141.101.118.159; 141.101.118.158)  
- Email: furkan@cod.com

**Sample redirection chain for the rogue social media distribution platform's core functions:**

*hxxp://profonixuser.net/new.php?nocache=1044379803*

->

*hxxp://sosyalmedyakusu.com/oauth.php*

(108.162.199.203;

108.162.198.203)

Email:

furkan@cod.com

->

*hxxp://hizliservis.pw/face.php*

->

*hxxp://socialhaberler.com/manyak.php ->*

*hxxp://profonixuser.net/new.php ->*

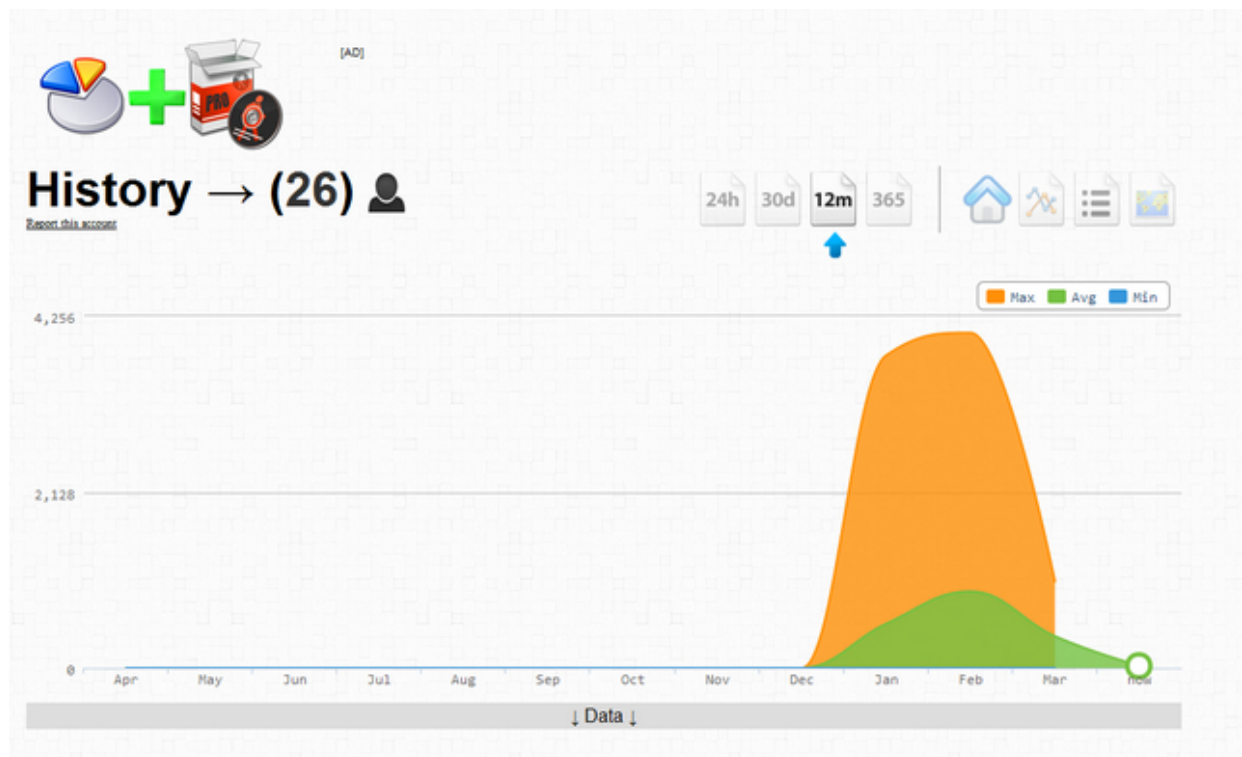
*hxxp://profonixuser.net/amk.php (141.101.117.218) ->*

*hxxp://me.cf/dhtcw (31.170.164.67) -> hxxps://video-players.herokuapp.com/?55517841177*

*(107.20.187.159) -> hxxp://kingprofonix.net/hxxp://kingprofonix.com (108.162.198.203) the same domain is also*

known to have responded to 108.162.197.62

862



**Related MD5s known to have phoned back to the same IP (108.162.198.203) in the past:**

**[6]MD5: 505f615f9e1c4fdc03964b36ec877d57**

**Sample internal redirectors structure:**

*hxxp://profonixuser.net/fb.php ->*

*hxxp://profonixuser.net/manyak.php ->*

*hxxp://molotofcu.com/google/hede.php (199.27.134.199)*

->

*hxxp://profonixuser.net/pp.php*

->

*hxxp://gdriv.es/awalbbmprtbpahpolcdt?jgxebgqjl*

->

*hxxps://googledrive.com/host/0B08vFK4UtN5kdjV2NkIHVTVjc  
TQ -> hxxp://sosyalmedyakusu.com/s3x.php?ref=g-*

*oogle*

*hxxp://profonixuser.net/user.php -> hxxp://goo.gl/ber2EP ->  
hxxps://buexe-x.googlecode.com/svn/FlashPlayer*

*%20Setup.exe -> [7]MD5:*

**60137c1cb77bed9afcbbbc3ad910df3f** -> phones back to  
**wjetphp.com** (46.105.56.61) **Secondary sample internal  
redirectors structure:**

*hxxp://profonixuser.net/yarak.txt*

->

*hxxp://profonixuser.net/u.exe*

->

*hxxp://profonixuser.net/yeni.txt*

-

>

*hxxp://profonixuser.net/yeni.exe*

->

*hxxp://profonixuser.net/recep.html*

->

*hxxp://goo.gl/ber2EP*

->

*hxxp://wjetphp.com/unlu/player.swf ->*

*hxxp://profonixuser.net/kral.txt -> hxxp://likef.in/fate.exe -*

108.162.194.123; 108.162.195.123; 108.162.199.107 -

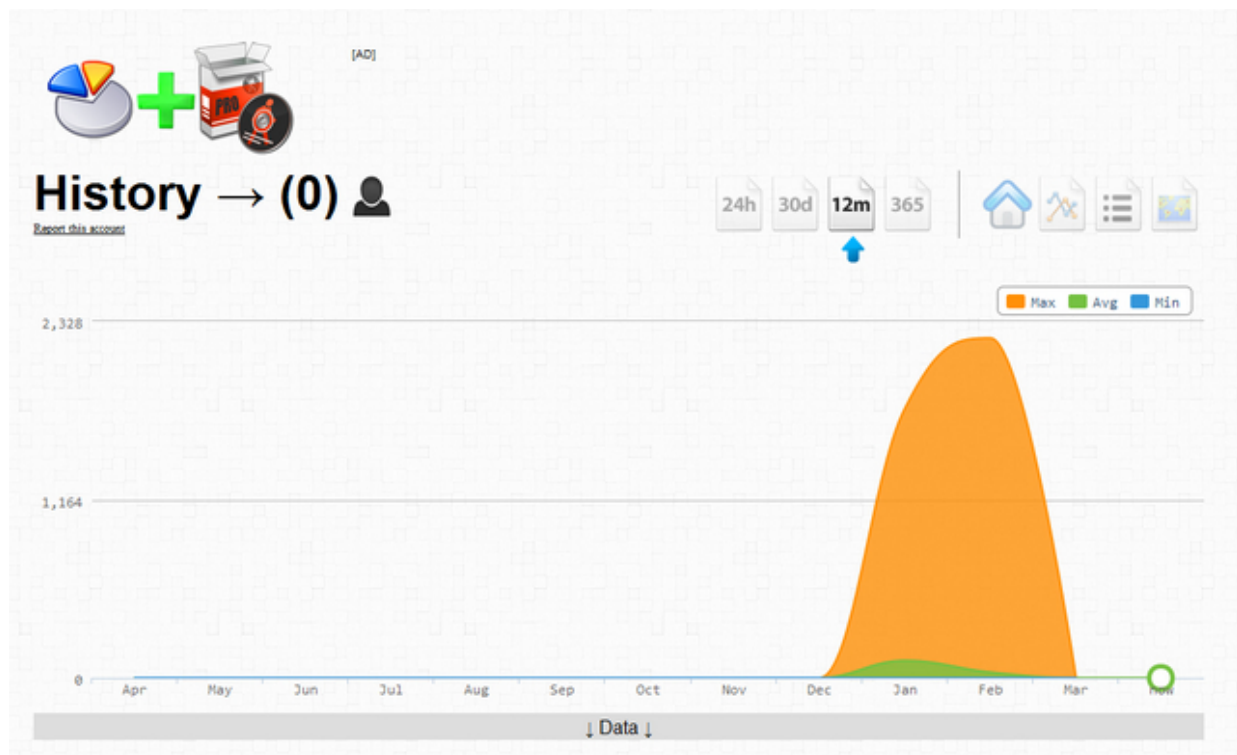
known to have phoned back to the same IP is also the

following malicious [8]**MD5:**

**effcfe91beaf7a3ed2f4ac79525c5fc5** - detected by 35  
out of 50 antivirus scanners as Trojan-

Ransom.Win32.Foreign.kcme

863



Once executed, the sample phones back to likef.biz (176.53.119.195). The same domain is also known to have responded to the following IPs 141.101.116.165; 141.101.117.165.

Here's comes the interesting part. The fine folks at [9]**ExposedBotnets**, have already intercepted a malicious

Facebook spreading campaign, that's using the already profiled in this post **videotr.in**.

Having directly connected the cybercrime-friendly SWF iframe/redirector injecting service, with **hizliservis.pw** as

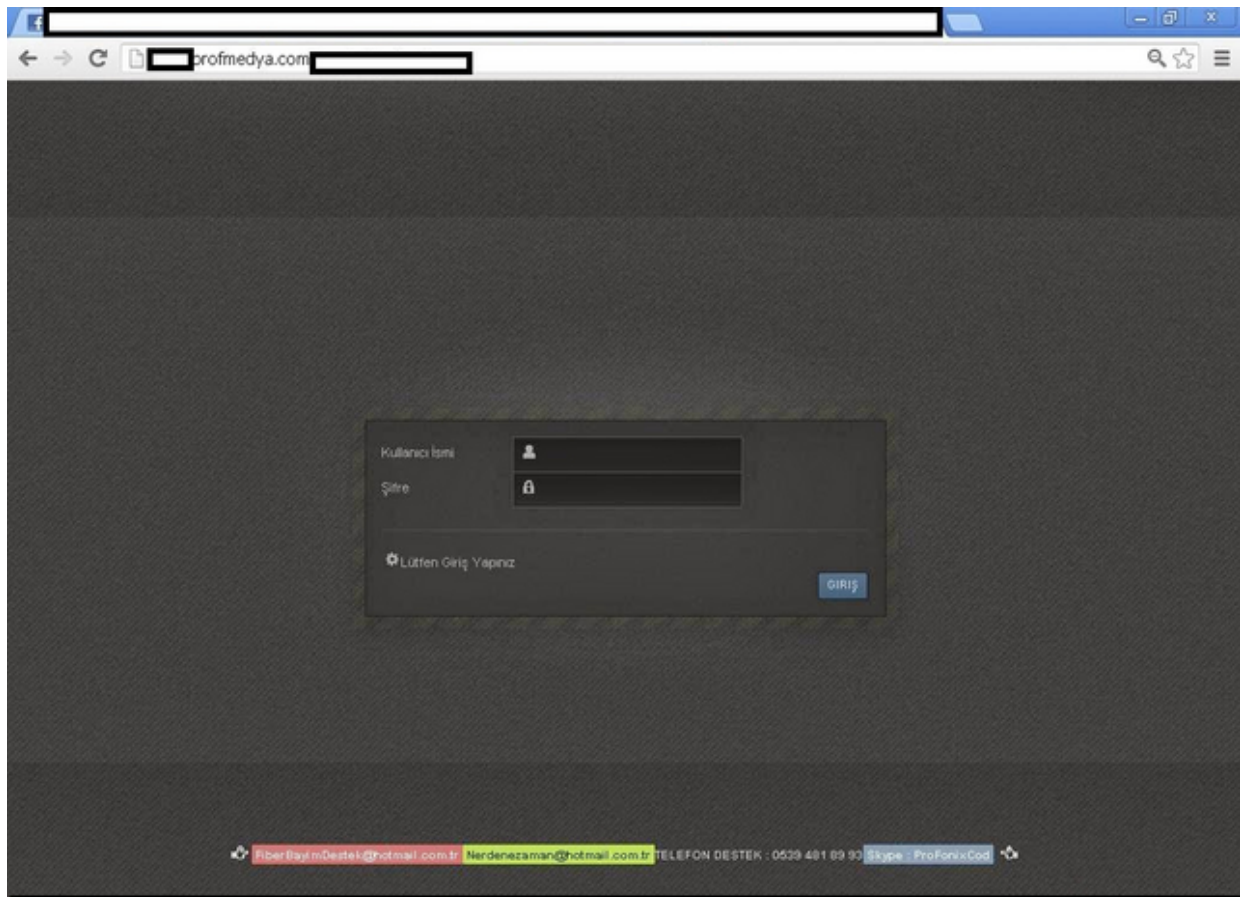
well as the SocialMediaSystem as being part of the same malicious infrastructure, it's time to profile the fraud-

ulent/malicious adversaries behind the campaigns. The cybercriminals behind these campaigns, appear to be

operating a rogue social media service, targeting Facebook Inc.

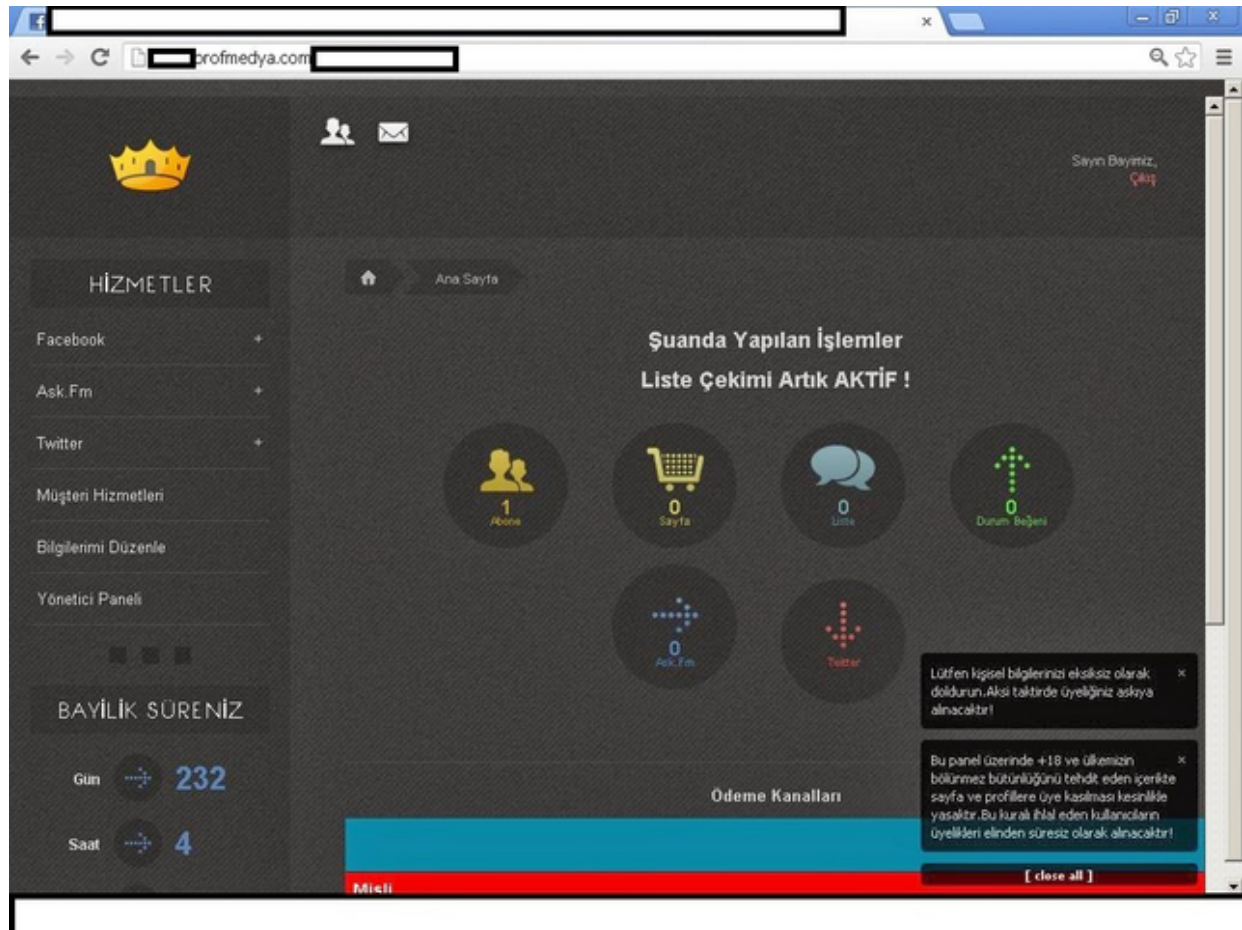
### **Sample screenshots of the social media distribution platform's Web based interface:**

864



865





**Sample advertisement of the rogue social media distribution platform:**

866

#### **Facebook Page Member Shooting !**

1K: 5\$  
2K: 10\$  
3K: 15\$  
4K: 20\$  
5K: 25\$  
  
10K: 50\$  
20K: 100\$  
30K: 150\$  
40K: 200\$  
50K: 250\$

#### **Facebook Subscriber Prices**

1K: 2\$  
2K: 5\$  
3K: 7\$  
4K: 10\$  
5K: 12\$  
6K: 13\$  
7K: 15\$  
8K: 17\$  
9K: 20\$  
10K: 25\$  
  
20K: 50\$  
30K: 100\$  
40K: 150\$  
50K: 200\$

#### **Facebook Lists Prices**

### **Facebook Lists Prices**

1K: 5\$  
2K: 10\$  
3K: 15\$  
4K: 20\$  
5K: 25\$  
6K: 30\$  
7K: 35\$  
8K: 40\$  
9K: 45\$  
10K: 50\$

20K: 50\$  
30K: 100\$  
40K: 150\$  
50K: 200\$

**Dealers For Sale ! ProfMedya**

**WebSite : [www.profmedya.com](http://www.profmedya.com)**

**Communication**

**Skype: Profonixcod**

**MSN: [FiberBayimDestek@hotmail.com.tr](mailto:FiberBayimDestek@hotmail.com.tr)**

**Skype ID of the rogue company: ProFonixcod**

**Secondary company name: ProfMedya -**

hxxp://profmedya.com - 178.33.42.254; 188.138.9.39;  
89.19.20.242 - Email:

kayahoca@gmail.com. The same domain, profmedya.com  
used to respond to 188.138.9.39.

**Domains known to have responded to the same IP (188.138.9.39) are also the following malicious domains:**

hxxp://faceboook.biz

hxxp://worldmedya.net

fhxxp://astotoliked.net

hxxp://adsmedya.com

hxxp://facebookmedya.biz

hxxp://fastotolike.com

hxxp://fbmedyahizmetleri.com

hxxp://fiberbayim.com

hxxp://profonixcoder.com

hxxp://sansurmedya.biz

hxxp://sosyalpaket.com

868

hxxp://takipciniarttir.net

hxxp://videomedya.net

hxxp://videopackage.biz

hxxp://worldmedya.net

hxxp://www-facebook.net

hxxp://www.facebook-java.com

hxxp://www.facemlike.com

hxxp://www.fastcekim.com

hxxp://www.fastotolike.com

hxxp://www.fbmedyahizmetleri.com

hxxp://www.profmedya.com

hxxp://www.sansurmedya.com

**Rogue social media distribution platform operator's name:** Fatih Konar

**Associated emails:** fiberbayimdestek@hotmail.com.tr;  
nerdenezaman@hotmail.com.tr

**Google+ Account:**

hxxps://plus.google.com/1038477436831294 39807/about

**Twitter account:** hxxps://twitter.com/ProfonixCodtr

**Domain name reconnaissance:**

profonixcod.com (profonix-cod.com) - 216.119.143.194 -  
Email: abazafamily \_@hotmail.com (related domains

known to have been registered with the same email -  
warningyoutube.com; likebayi.com)

profonixcod.net

Updated will be posted as soon as new developments take place.

1. <http://ddanchev.blogspot.com/2014/01/facebook-spreading-amazon.html>

2. <http://www.webroot.com/blog/2014/02/14/doubleclick-malvertising-campaign-exposes-long-run-beneath-radar-malvertising-infrastructure/>
3. <http://www.webroot.com/blog/2013/06/03/compromised-ftpssh-account-privilege-escalating-mass-iframe-embedding-platform-released-on-the-underground-marketplace/>
4. <http://www.webroot.com/blog/2012/11/26/cybercriminals-release-stealthy-diy-mass-iframe-injecting-apache-2-modules/>
5. <https://www.virustotal.com/en/file/7f7bd5f002de9aedde4fa5dca5356cf576c95eb58bd85178d0781dfc0a1a6ca4/analysis/1395436639/>
6. <https://www.virustotal.com/en/file/7aae8f81397608d3c08e3fb645c4001260f560f1470bfbfd00ed08cde8ceaedc8/analysis/>
7. <https://www.virustotal.com/en/file/4b91da4289b8765d4646176b7fa21f8de515ba02e97519589452346d54ff2204/analysis/>
8. <https://www.virustotal.com/en/file/a50411aa3850e1defcce38f079daf175a9ca7fb32749c9b4394ef6236476d094/analysis/>

9. <http://www.exposedbotnets.com/2014/01/videotrin-facebook-spreading-browser.html>

869


2.2


March


870


## Webroot Threat Blog

Internet Security Threat Updates & Insights

 **READ**  
Webroot Blogs

 **WATCH**  
Webroot Vlogs

 **CONNECT**  
Meet The Threat Team

 **DISCUSS**  
Webroot Community

Search for:

Please select your language from below. Translation services provided by Google.



**Our Extended Community**



**Top Authors**

 Dancho Danchev

 Grayson Milbourne

 Nathan Collier

 Tyler Moffitt

 Brenden Vaughan

## **Summarizing Webroot's Threat Blog Posts for January (2014-03-06 19:41)**

The following is a brief summary of all of my posts at [1]**Webroot's Threat Blog** for January, 2014. You can subscribe to [2]**Webroot's Threat Blog RSS Feed**, or follow me on Twitter:

**01.** [3]'Adobe License Service Center Order NR' and 'Notice to appear in court' themed malicious spam campaigns

intercepted in the wild

**02.** [4]New "Windows 8 Home Screen" themed passwords/game keys stealer spotted in the wild

**03.** [5]Vendor of TDoS products resets market life cycle of well known 3G USB modem/GSM/SIM card-based TDoS

tool

**04.** [6]New TDoS market segment entrant introduces 96 SIM cards compatible custom GSM module, positions itself

as market disruptor

**05.** [7]DIY Python-based mass insecure WordPress scanning/exploiting tool with hundreds of pre-defined exploits

871

spotted in the wild

**06.** [8]Google's reCAPTCHA under automatic fire from a newly launched reCAPTCHA-solving/breaking service

**07.** [9]Fully automated, API-supporting service, undermines Facebook and Google's 'SMS/Mobile number activation'



account registration process

**08.** [10]Newly launched managed 'compromised/hacked accounts E-shop hosting as service' standardizes the monetization process

**09.** [11]Newly released Web based DDoS/Passwords stealing-capable DIY botnet generating tool spotted in the wild

**10.** [12]Cybercriminals release new Web based keylogging system, rely on penetration pricing to gain market share

***This post has been reproduced from [13]Dancho Danchev's blog . Follow him [14]on Twitter.***

1. <http://www.webroot.com/blog>
2. <http://feeds2.feedburner.com/WebrootThreatBlog>
3. <http://www.webroot.com/blog/2014/01/07/adobe-license-service-center-order-nr-notice-appear-court-themed-malicious-spam-campaigns-intercepted-wild/>
4. <http://www.webroot.com/blog/2014/01/09/new-windows-8-home-screen-themed-passwordgame-keys-stealer-spotted-wild/>
5. <http://www.webroot.com/blog/2014/01/13/vendor-tdos-products-releases-new-gsm3g-usb-modem-based-tdos-tool/>
6. <http://www.webroot.com/blog/2014/01/16/new-tdos-market-segment-entrant-introduces-96-sim-cards-compatible-custom-gsm-module-positions-market-disruptor/>

7. <http://www.webroot.com/blog/2014/01/17/diy-python-based-mass-insecure-wordpress-scanningexploiting-tool-hundreds-pre-defined-exploits-spotted-wild/>

8.

<http://www.webroot.com/blog/2014/01/21/googles-recaptcha-automatic-fire-newly-launched-recaptcha-solving-breaking-service/>

9. <http://www.webroot.com/blog/2014/01/22/fully-automated-api-supporting-service-undermines-facebook-google>

[-sms-activation-mobile-number-activation-account-regist](http://www.webroot.com/blog/2014/01/22/fully-automated-api-supporting-service-undermines-facebook-google)

10. <http://www.webroot.com/blog/2014/01/24/newly-launched-managed-compromisedhacked-accounts-e-shop-hosting-s>

[ervice-standardizes-monetization-process/](http://www.webroot.com/blog/2014/01/24/newly-launched-managed-compromisedhacked-accounts-e-shop-hosting-s)

11. <http://www.webroot.com/blog/2014/01/30/newly-released-web-based-ddospasswords-stealing-capable-diy-botnet>

[-generating-tool-spotted-wild/](http://www.webroot.com/blog/2014/01/30/newly-released-web-based-ddospasswords-stealing-capable-diy-botnet)

12.


<http://www.webroot.com/blog/2014/01/31/cybercriminals-release-new-web-based-keylogging-system/>


13. <http://ddanchev.blogspot.com/>


14. <http://twitter.com/danchodanchev>


## Webroot Threat Blog

Internet Security Threat Updates & Insights



**READ**  
Webroot Blogs



**WATCH**  
Webroot Vlogs


**CONNECT**  
Meet The Threat Team







**DISCUSS**  
Webroot Community

Search for:

Please select your language from below. Translation services provided by Google.  


**Our Extended Community**  


**Top Authors**

-  Dancho Danchev
-  Grayson Milbourne
-  Nathan Collier
-  Tyler Moffitt
-  Brenden Vaughan

### Can Security Survive in an Increasingly Insecure World?

February 21st, 2014 by [Grayson Milbourne](#)

2013 was not a good year in terms of cyber security. Despite companies spending an increasingly significant percent of revenue on security technology – systems designed to thwart, detect and prevent hackers from gaining access to their networks and sensitive data – attacks continue to succeed. Recently, the trend has shifted to attacking point of sale (POS) systems. While Target is the largest example, similar attacks have occurred in industries ranging from department stores to hospitals to hotel chains. Basically anywhere large scale financial transactions take place. The focus on POS systems doesn't come as a surprise. Cybercriminals have always [...]

[CONTINUE READING >](#)

Posted in: [Deep Knowledge](#), [malware](#), [Mobile](#), [Threat Research](#)

Tagged: [cyber security](#) [deep threat knowledge](#) [RSA](#) [RSA Conference](#) [RSAC](#) [security](#) [survival](#)

### Spamvertised 'You received a new message from Skype voicemail service' themed emails lead to Angler exploit kit

February 20th, 2014 by [Dancho Danchev](#)

We've just intercepted a currently circulating malicious spam campaign that's attempting to trick potential botnet victims into thinking that they've received a legitimate Voice Message Notification from Skype. In reality though, once socially engineered users click on the malicious link found in the bogus emails, they're automatically exposed to the Angler exploit kit. More details...

X

## Summarizing Webroot's Threat Blog Posts for February (2014-03-06 20:48)

The following is a brief summary of all of my posts at [1]**Webroot's Threat Blog** for February, 2014. You can subscribe to [2]**Webroot's Threat Blog RSS Feed**, or follow me on Twitter:

- 01.** [3]Cybercriminals release Socks4/Socks5 based Alexa PageRank boosting application
- 02.** [4]Market leading 'standardized cybercrime-friendly E-shop' service brings 2500+ boutique E-shops online
- 03.** [5]Managed TeamViewer based anti-forensics capable virtual machines offered as a service
- 04.** [6]Malicious campaign relies on rogue WordPress sites, leads to client-side exploits through the Magnitude exploit kit
- 05.** [7]'Hacking for hire' teams occupy multiple underground market segments, monetize their malicious 'know how'
- 06.** [8]DoubleClick malvertising campaign exposes long-run beneath the radar malvertising infrastructure
- 07.** [9]Spamvertised 'Image has been sent' Evernote themed campaign serves client-side exploits
- 08.** [10]Spamvertised 'You received a new message from Skype voicemail service' themed emails lead to Angler

873

exploit kit

***This post has been reproduced from [11]Dancho Danchev's blog . Follow him [12]on Twitter.***

- 1. <http://www.webroot.com/blog>
- 2. <http://feeds2.feedburner.com/WebrootThreatBlog>
- 3.

<http://www.webroot.com/blog/2014/02/04/cybercriminals-release-socks4socks5-based-alexa-pagerank-boosting-application/>

4. <http://www.webroot.com/blog/2014/02/07/market-leading-standardized-cybercrime-friendly-e-shop-service-brings-2500-boutique-e-shops-online/>

5. <http://www.webroot.com/blog/2014/02/10/managed-teamviewer-based-anti-forensics-capable-virtual-machines-offered-service/>

6. <http://www.webroot.com/blog/2014/02/12/rogue-wordpress-sites-lead-to-client-side-exploits/>

7. <http://www.webroot.com/blog/2014/02/13/hacking-hire-teams-occupy-multiple-underground-market-segments-monetize-malicious-know/>

8. <http://www.webroot.com/blog/2014/02/14/doubleclick-malvertising-campaign-exposes-long-run-beneath-radar-malvertising-infrastructure/>

9. <http://www.webroot.com/blog/2014/02/18/spamvertised-image-sent-evernote-themed-campaign-serves-client-side-exploits/>

10. <http://www.webroot.com/blog/2014/02/20/spamvertised-received-new-message-skype-voicemail-service-themed-emails-lead-angler-exploit-kit/>

11. <http://ddanchev.blogspot.com/>

12. <http://twitter.com/danchodanchev>

874

Şuan sitedeki 985 kişi toplam 3,457 video'nun keyfini çıkarıyor.. Sizde onlardan birisi olun!

- [kayıt ol](#)
- [giriş yap](#)
- [anasayfa](#)
- [kategoriler](#)
- [kanallar](#)

### # Recep İvedik 4 ( Full İzle - HD Ücretsiz )

Please install Flash Player...

1 gün önce eklendi

15,547 kez izlendi

Paylaş:

[Video](#)

© 2011 - [unluvideolari.info](http://unluvideolari.info)

- Hızlı Menü
- [anasayfa](#)
- [hakkımızda](#)
- [kategoriler](#)
- [kanallar](#)
- [sss](#)
- [iletişim](#)
- Sosyal Ağlar
- [Facebook Sayfamız](#)
- [Twitter'dan Takip Edin!](#)
- [Videolara Abone Olun!](#)
- [İletişime Geçin!](#)

## Win32.Nixofro Serving, Malicious Infrastructure, Exposes Fraudulent Facebook Social Media Service

### Provider (2014-03-22 08:18)

I've recently spotted a malicious, cybercrime-friendly SWF iframe/redirector injecting service, that also exposes a

long-run Win32.Nixofro serving malicious infrastructure, currently utilized for the purpose of operating a rogue social

media service provider, that's targeting Turkish Facebook users through the ubiquitous social engineering vector, for

such type of campaigns, namely, the fake Adobe Flash player.

Let's profile the service, discuss its relevance in the broader context of the threat landscape, provide action-

able/historical threat intelligence on the malicious infrastructure, the rogue domains involved in it, the malicious

MD5s served by the cybercriminals behind it, and directly link it to a [1]**previously profiled Facebook spreading**

**P2P-Worm.Win32.Palevo serving campaign.**

The managed SWF iframe/redirector service, is a great example of a cybercrime-as-a-service type of underground

market proposition, empowering, both, sophisticated and novice cybercriminals with the necessary ([2]**malvertising**)

'know-how', in an efficient manner, directly intersecting with the commercial availability of [3]**sophisticated mass**

**Web site/[4]Web server** malicious script embedding platforms.

The managed SWF iframe/redirector injecting service is currently responding to 108.162.197.62 and 108.162.196.62

|                 | Обычный | Оптовый | VIP персона |
|-----------------|---------|---------|-------------|
| Неделя (7 дней) | 5       | 1       | 0.5         |
| Месяц (30 дней) | 10      | 2       | 1           |
| Год (365 дней)  | 15      | 5       | 2           |

Known to have responded to the same IPs (108.162.197.62; 108.162.196.62) is also a key part of the malicious

infrastructure that I'll expose in this post, namely **hizliservis.pw** - Email: furkan@cod.com.

**Known to have phoned back to the same IP (108.162.197.62) are also the following malicious MD5s:**

MD5: 432efe0fa88d2a9e191cb95fa88e7b36

MD5: 720ecb1cf4f28663f4ab25eedf620341

MD5: 02691863e9dfb9e69b68f5fca932e729

MD5: 69ed70a82cb35a454c60c501025415aa

MD5: cc586a176668ceef14891b15e1b412ab

MD5: 74291941bddcec131c8c6d531fcb1886

MD5: 7c27d9ff25fc40119480e4fe2c7ca987

MD5: 72c030db7163a7a7bf2871a449d4ea3c

MD5: 432efe0fa88d2a9e191cb95fa88e7b36

**Known to have phoned to the same IP (108.162.196.62) are also the following malicious MD5s:**

MD5: eda3f015204e9565c779e0725915864f



MD5: effcfe91beaf7a3ed2f4ac79525c5fc5

MD5: 14acd831691173ced830f4b51a93e1ca

MD5: 7f93b0c611f7020d28f7a545847b51e0

MD5: bcfce3a9bf2c87dab806623154d49f10

MD5: 4c90a89396d4109d8e4e2491c5da4846

MD5: 289c4f925fdec861c7f765a65b7270af

### **Sample redirection chain leading to the fake Adobe Flash Player:**

*hxxp://hizliservis.pw/unlu.htm*

->

*hxxp://hizliservis.pw/indir.php*

->

*hxxp://unluvideolari.info*

->

*hxxp://videotr.in/player.swf*

->

*hxxp://izleyelim.s3.amazonaws.com/movie.mp4*

*&skin=newtubedark/NewTubeDark.xml &streamer=lighttpd  
&image=hqdefault.jpg*

### **Domain name reconnaissance:**

hizliservis.pw - Email: furkan@cod.com

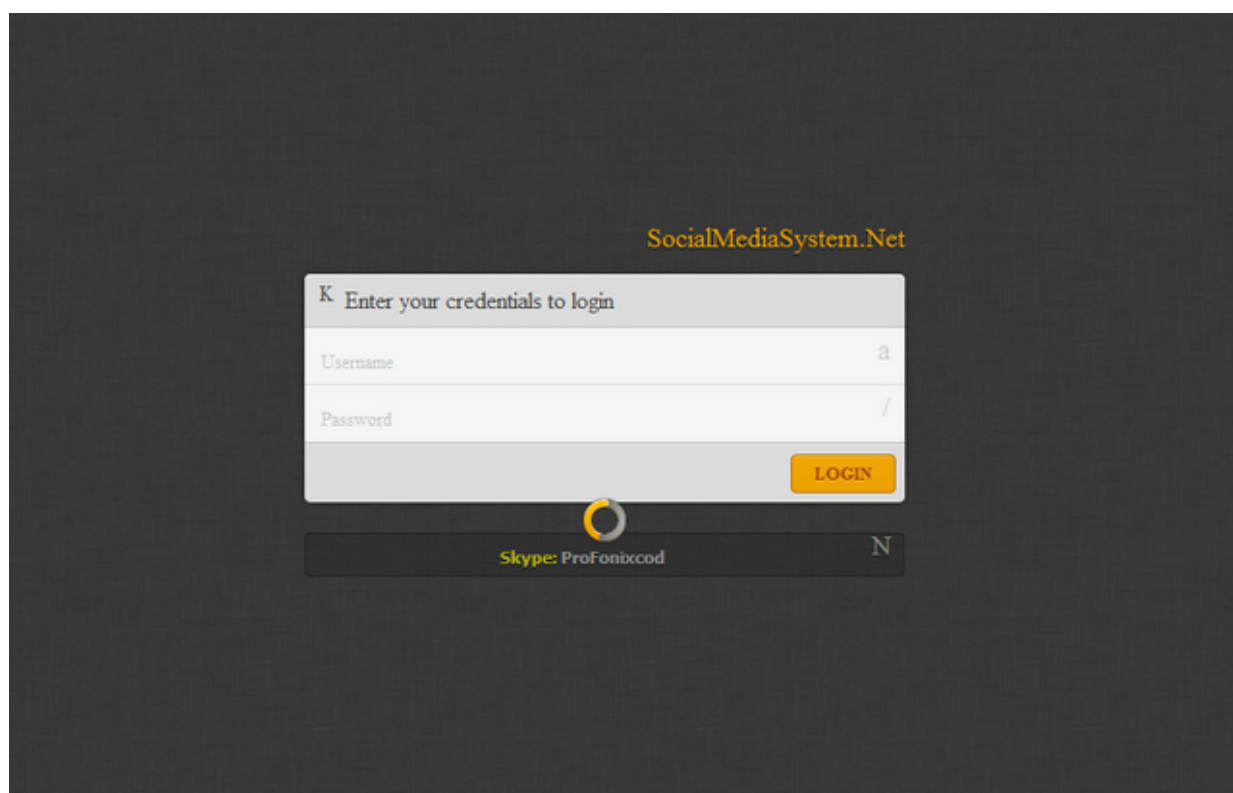
videotr.in - Email: tiiknet@yandex.com; snack@log-z.com

izleyelim.s3.amazonaws.com - 176.32.97.249

Within **hizliservis.pw**, we can easily spot yet another part of the same malicious/fraudulent infrastructure,

namely, the rogue social media distribution platform's login interface.

876

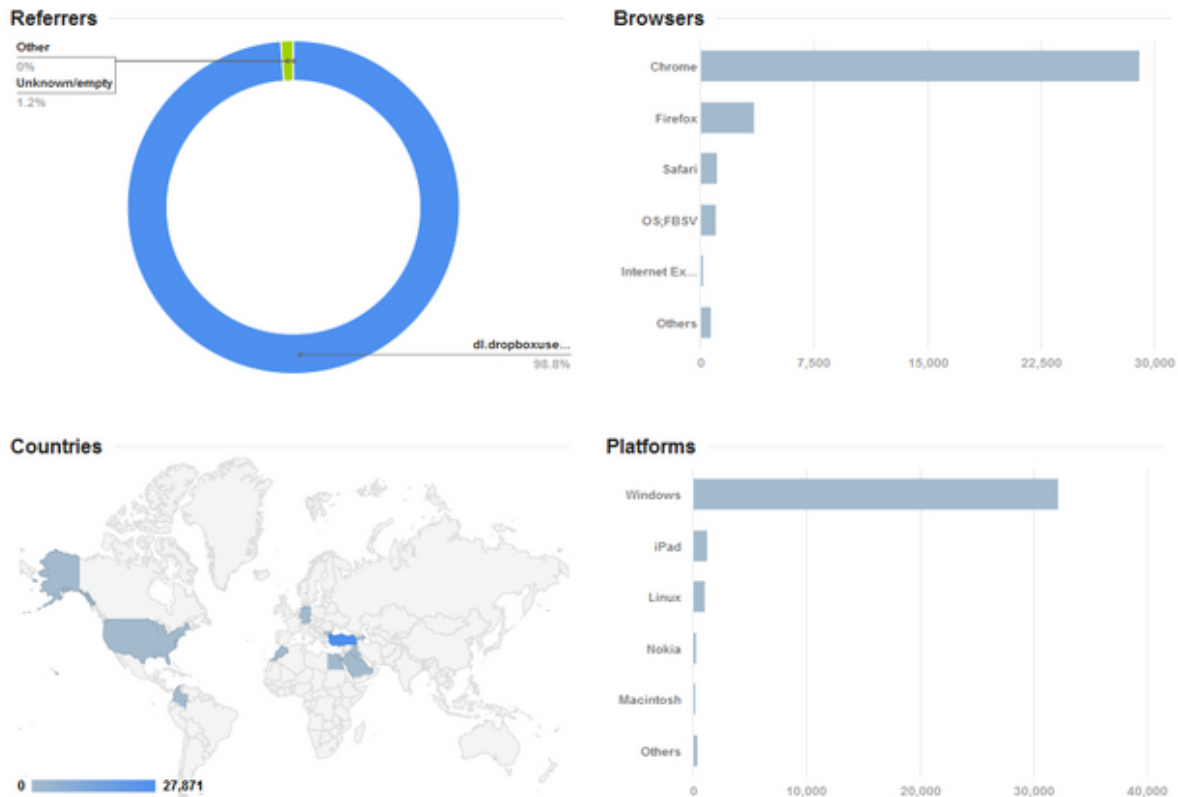




**Sample redirection chain leading to a currently active fake Adobe Flash Player (Win32.Nixofro):**

hxxp://socialmediasystem.net/down.php ->  
hxxps://profonixback31.googlecode.com/svn/FlashPlayer  
\_Guncelle.exe

877



## Detection rate for the fake Adobe Flash Player:

[5]**MD5: 28c3c503d398914bdd2c2b3fdc1f9ea4** - detected by 36 out of 50 antivirus scanners as Win32.Nixofro

Once executed, the sample phones back to **profonixuser.net** (141.101.117.218)

**Known to have responded to the same IP (141.101.117.218) are also the following malicious MD5s:**

MD5: 53360155012d8e5c648aca277cbde587

MD5: a66a1c42cc6fb775254cf32c8db7ad5b

MD5: a051fd83fc8577b00d8d925581af1a3b

MD5: f47784817a8a04284af4b602c7719cb7

MD5: 2e5c75318275844ce0ff7028908e8fb4

MD5: 90205a9740df5825ce80229ca105b9e8

**Domain name reconnaissance for the rogue social media distribution platform:**

socialmediasystem.Net (141.101.118.159; 141.101.118.158)  
- Email: furkan@cod.com

**Sample redirection chain for the rogue social media distribution platform's core functions:**

*hxxp://profonixuser.net/new.php?nocache=1044379803*

->

*hxxp://sosyalmedyakusu.com/oauth.php*

(108.162.199.203;

108.162.198.203)

Email:

furkan@cod.com

->

*hxxp://hizliservis.pw/face.php*

->

*hxxp://socialhaberler.com/manyak.php ->*

*hxxp://profonixuser.net/new.php ->*

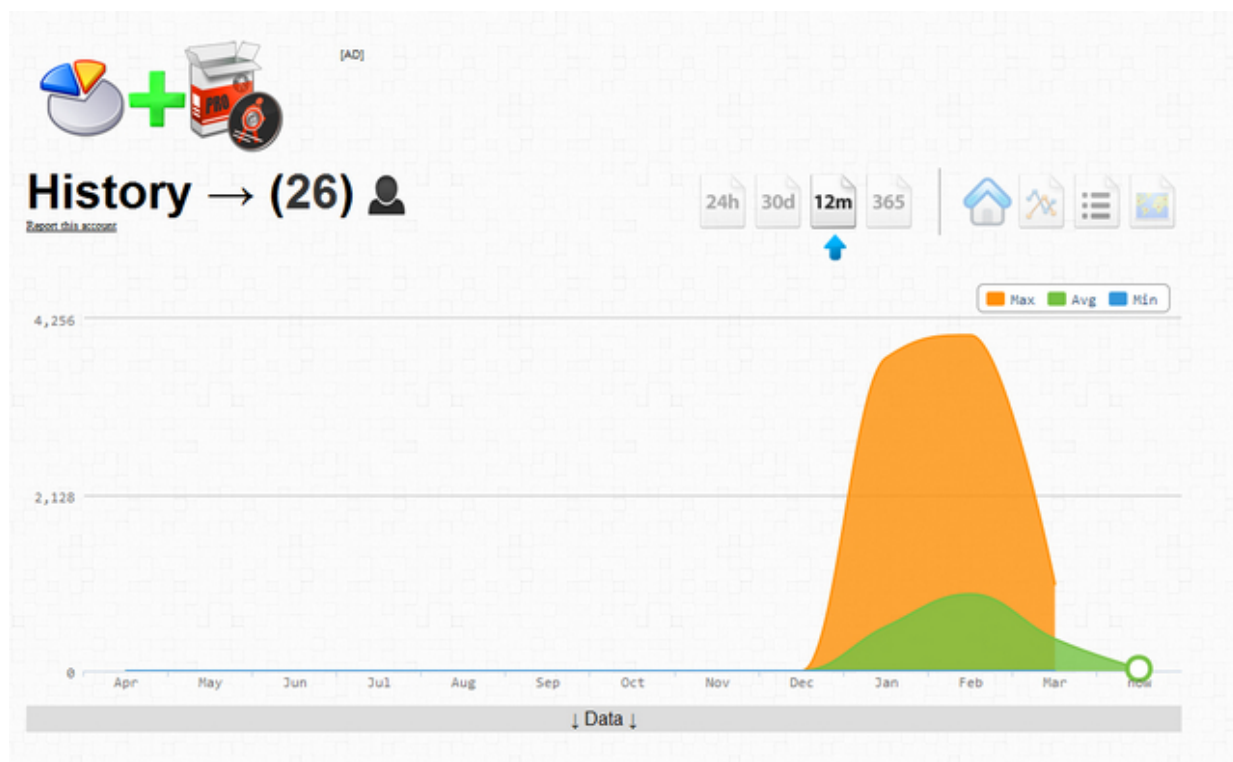
*hxxp://profonixuser.net/amk.php (141.101.117.218) ->*

*hxxp://me.cf/dhtcw (31.170.164.67) -> hxxps://video-players.herokuapp.com/?55517841177*

(107.20.187.159) -> *hxxp://kingprofonix.net/hxxp://kingprofonix.com* (108.162.198.203) the same domain is also

known to have responded to 108.162.197.62

878



**Related MD5s known to have phoned back to the same IP (108.162.198.203) in the past:**

**[6]MD5: 505f615f9e1c4fdc03964b36ec877d57**

**Sample internal redirectors structure:**

*hxxp://profonixuser.net/fb.php ->*

*hxxp://profonixuser.net/manyak.php ->*

*hxxp://molotofcu.com/google/hede.php* (199.27.134.199)

->

*hxxp://profonixuser.net/pp.php*

->

*hxxp://gdriv.es/awalbbmprtbpahpolcdt?jgxebgqjl*

->

*hxxps://googledrive.com/host/0B08vFK4UtN5kdjV2NklHVTVjc  
TQ -> hxxp://sosyalmedyakusu.com/s3x.php?ref=g-*

*oogle*

*hxxp://profonixuser.net/user.php -> hxxp://goo.gl/ber2EP ->  
hxxps://buexe-x.googlecode.com/svn/FlashPlayer*

*%20Setup.exe -> [7]MD5:*

**60137c1cb77bed9afcbbbc3ad910df3f** -> phones back to  
**wjetphp.com** (46.105.56.61) **Secondary sample internal  
redirectors structure:**

*hxxp://profonixuser.net/yarak.txt*

->

*hxxp://profonixuser.net/u.exe*

->

*hxxp://profonixuser.net/yeni.txt*

-

>

*hxxp://profonixuser.net/yeni.exe*

->

*hxxp://profonixuser.net/recep.html*

->

*hxxp://goo.gl/ber2EP*

->

*hxxp://wjetphp.com/unlu/player.swf* ->

*hxxp://profonixuser.net/kral.txt* -> *hxxp://likef.in/fate.exe* -

108.162.194.123; 108.162.195.123; 108.162.199.107 -

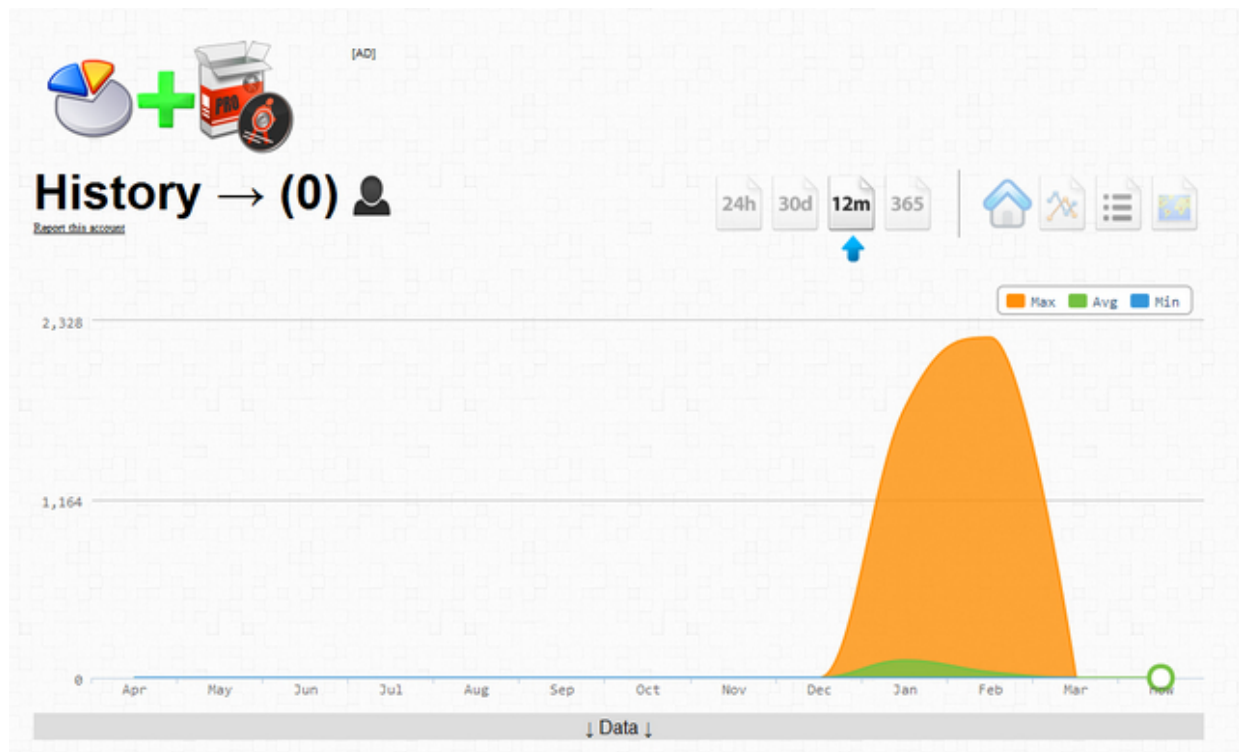
known to have phoned back to the same IP is also the

following malicious [8]**MD5:**

**effcfe91beaf7a3ed2f4ac79525c5fc5** - detected by 35 out of 50 antivirus scanners as Trojan-

Ransom.Win32.Foreign.kcme

879





Once executed, the sample phones back to likef.biz (176.53.119.195). The same domain is also known to have

responded to the following IPs 141.101.116.165; 141.101.117.165.

Here's comes the interesting part. The fine folks at [9]**ExposedBotnets**, have already intercepted a malicious

Facebook spreading campaign, that's using the already profiled in this post **videotr.in**.

Having directly connected the cybercrime-friendly SWF iframe/redirector injecting service, with **hizliservis.pw** as

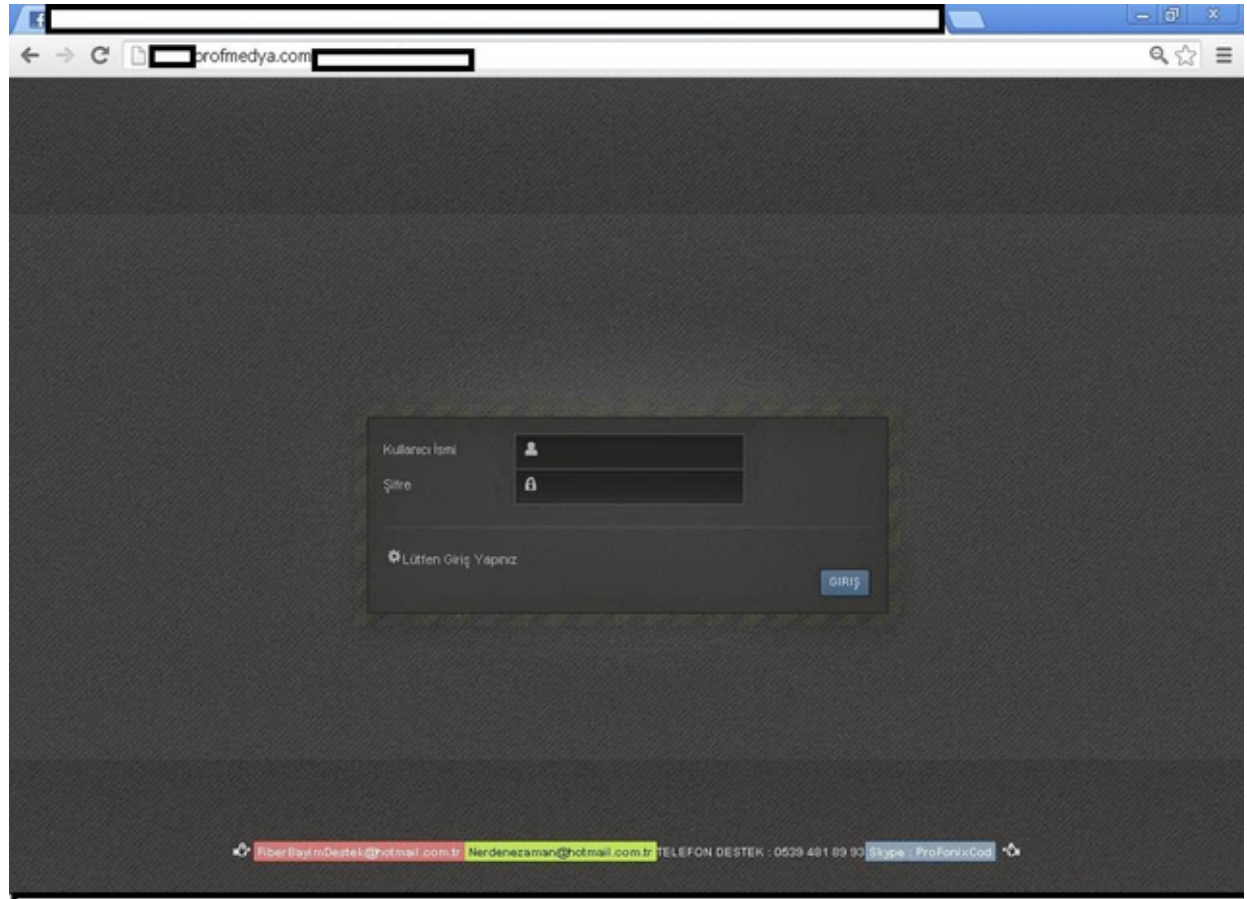
well as the SocialMediaSystem as being part of the same malicious infrastructure, it's time to profile the fraud-

ulent/malicious adversaries behind the campaigns. The cybercriminals behind these campaigns, appear to be

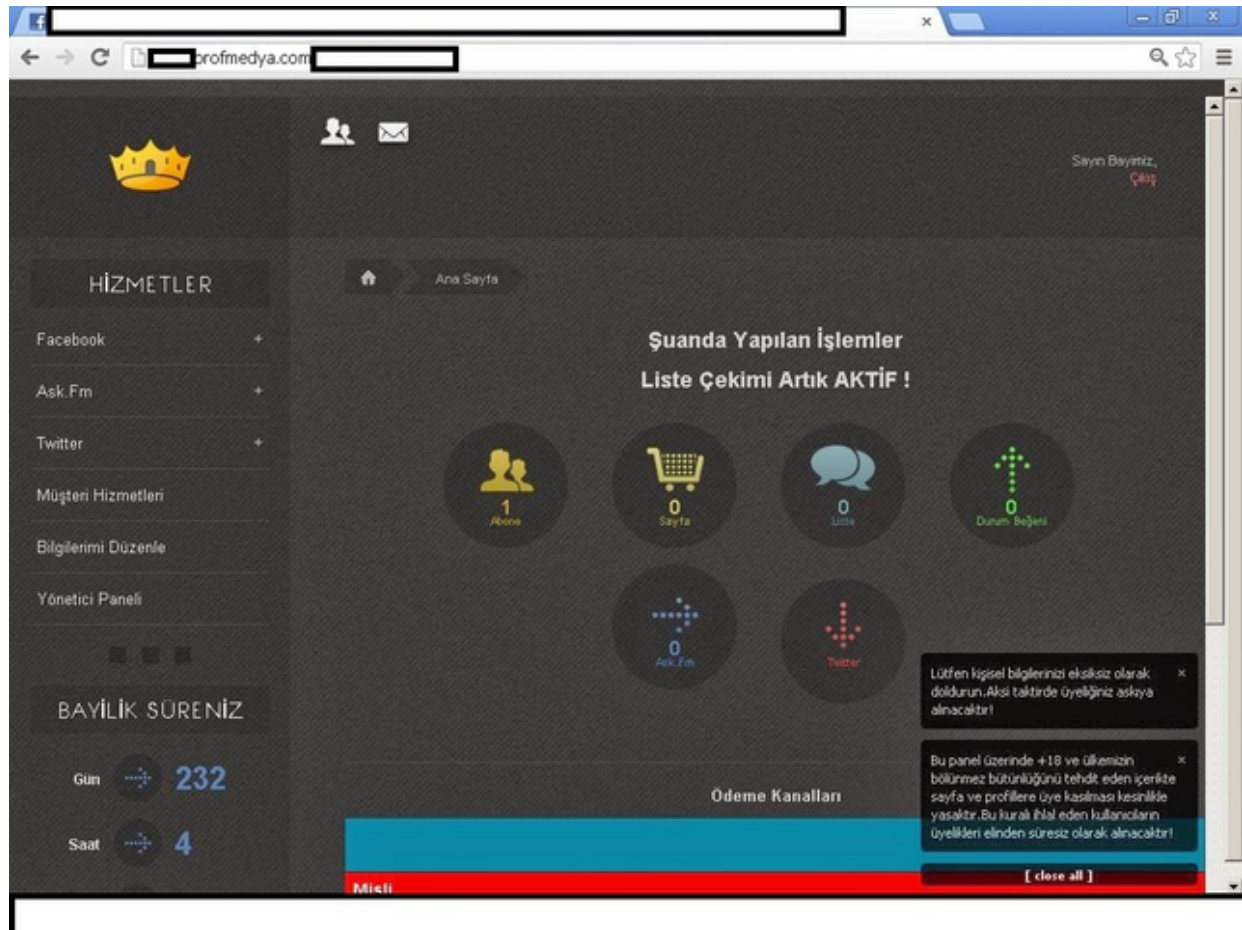
operating a rogue social media service, targeting Facebook Inc.

**Sample screenshots of the social media distribution platform's Web based interface:**

880



881



**Sample advertisement of the rogue social media distribution platform:**

882

#### Facebook Page Member Shooting !

1K: 5\$  
2K: 10\$  
3K: 15\$  
4K: 20\$  
5K: 25\$  
  
10K: 50\$  
20K: 100\$  
30K: 150\$  
40K: 200\$  
50K: 250\$

#### Facebook Subscriber Prices

1K: 2\$  
2K: 5\$  
3K: 7\$  
4K: 10\$  
5K: 12\$  
6K: 13\$  
7K: 15\$  
8K: 17\$  
9K: 20\$  
10K: 25\$  
  
20K: 50\$  
30K: 100\$  
40K: 150\$  
50K: 200\$

#### Facebook Lists Prices

883



**Skype ID of the rogue company:** ProFonixcod

**Secondary company name:** ProfMedya -  
hxxp://profmedya.com - 178.33.42.254; 188.138.9.39;  
89.19.20.242 - Email:

kayahoca@gmail.com. The same domain, profmedya.com used to respond to 188.138.9.39.

**Domains known to have responded to the same IP (188.138.9.39) are also the following malicious domains:**

hxxp://faceboook.biz

hxxp://worldmedya.net

fhxxp://astotoliked.net

hxxp://adsmedya.com

hxxp://facebookmedya.biz

hxxp://fastotolike.com

hxxp://fbmedyahizmetleri.com

hxxp://fiberbayim.com

hxxp://profonixcoder.com

hxxp://sansurmedya.biz

hxxp://sosyalpaket.com

884

hxxp://takipciniarttir.net

hxxp://videomedya.net

hxxp://videopackage.biz

hxxp://worldmedya.net

hxxp://www-facebook.net

hxxp://www.facebook-java.com

hxxp://www.facemlike.com

hxxp://www.fastcekim.com

hxxp://www.fastotolike.com

hxxp://www.fbmedyahizmetleri.com

hxxp://www.profmedya.com

hxxp://www.sansurmedya.com

**Rogue social media distribution platform operator's name:** Fatih Konar

**Associated emails:** fiberbayimdestek@hotmail.com.tr;  
nerdenezaman@hotmail.com.tr

**Google+ Account:**

hxxps://plus.google.com/1038477436831294 39807/about

**Twitter account:** hxxps://twitter.com/ProfonixCodtr

**Domain name reconnaissance:**

profonixcod.com (profonix-cod.com) - 216.119.143.194 -  
Email: abazafamily \_@hotmail.com (related domains

known to have been registered with the same email -  
warningyoutube.com; likebayi.com)

profonixcod.net

Updated will be posted as soon as new developments take place.

1. <http://ddanchev.blogspot.com/2014/01/facebook-spreading-amazon.html>
2. <http://www.webroot.com/blog/2014/02/14/doubleclick-malvertising-campaign-exposes-long-run-beneath-radar-malvertising-infrastructure/>
3. <http://www.webroot.com/blog/2013/06/03/compromised-ftpssh-account-privilege-escalating-mass-iframe-embedding-platform-released-on-the-underground-marketplace/>
4. <http://www.webroot.com/blog/2012/11/26/cybercriminals-release-stealthy-diy-mass-iframe-injecting-apache-2-modules/>
5. <https://www.virustotal.com/en/file/7f7bd5f002de9aedde4fa5dca5356cf576c95eb58bd85178d0781dfc0a1a6ca4/analysis/1395436639/>
6. <https://www.virustotal.com/en/file/7aae8f81397608d3c08e3fb645c4001260f560f1470bfbfd00ed08cde8ceaedc8/analysis/>
7. <https://www.virustotal.com/en/file/4b91da4289b8765d4646176b7fa21f8de515ba02e97519589452346d54ff2204/analysis/>
8. <https://www.virustotal.com/en/file/a50411aa3850e1defccea38>

[f079daf175a9ca7fb32749c9b4394ef6236476d094/analysis/](http://f079daf175a9ca7fb32749c9b4394ef6236476d094/analysis/)

9. <http://www.exposedbotnets.com/2014/01/videotrin-facebook-spreading-browser.html>

885

2.3

**October**

886



### **Rogue Android Apps Hosting Web Site Exposes Malicious Infrastructure (2014-10-21 21:24)**

With cybercriminals continuing to populate the cybercrime ecosystem with automatically generated and monetized

mobile malware variants, we continue to observe a logical shift towards convergence of [1]**cybercrime-friendly**

**revenue sharing affiliate networks**, and [2]**malicious infrastructure providers**, on their way to further achieve a positive ROI (return on investment) out of their [3]**risk-forwarding fraudulent activities**.

I've recently spotted a legitimately looking, [4]**rogue Android apps hosting Web site**, directly connected to a

market leading [5]**DIY API-enabled mobile malware generating/monetizing platform**, further exposing related



[6]**fraudulent operations**, performed, while utilizing the  
[7]**malicious infrastructure**, which I'll expose in this post.

Let's assess the campaign, expose the malicious infrastructure behind it, list the cybercrime-friendly premium rate SMS numbers, involved in it, as well as related malicious MD5s, known to have participated in the campaign/have utilized the same malicious infrastructure.

887

**Sample rogue Android apps hosting URL:**

*hxxp://androidapps.mob.wf - 37.1.206.173*

**Responding to the same IP (37.1.206.173) are also the following fraudulent domains:**

*hxxp://22-minuty.ru*

*hxxp://nygolfpro.com*

*hxxp://bloomster.dp.ua*

*hxxp://stdstudio.com.ua*

*hxxp://autosolnce.ru*

**Detection rate for sample rogue Android apps:**

[8]MD5: 4bf349b601fd73c74eafc01ce8ea8be7

[9]MD5: c4508c127029571e5b6f6b08e5c91415

[10]MD5: bd296d35bf41b9ae73ed816cc7c4c38b

**Sample**

**redirection**

**chain**

**exposing**

**the**

**fraudulent**

**infrastructure:**

*hxxp://22-minuty.ru*

->

*hxxp://playersharks2.com/player.php/?userid= -  
94.242.214.133; 94.242.214.155*

**Known to have responded to the same IPs  
(94.242.214.133; 94.242.214.155) are also the  
following fraudu-**

**lent domains, participating in a related revenue-  
sharing affiliate network based type of monetization  
scheme:**

*hxxp://4books.ru*

*hxxp://annoncer.media-bar.ru*

*hxxp://booksbutton1.com*

*hxxp://film-club.ru*

*hxxp://film-popcorn.ru*

*hxxp://filmbuttons.ru*

*hxxp://filmi-doma.com*

*hxxp://filmonika.ru*

*hxxp://films.909.su*

*hxxp://indiiskie.ru*

*hxxp://kinozond.ru*

*hxxp://media-bar.ru*

*hxxp://playersharks2.com*

*hxxp://playersharks4.com*

*hxxp://pplayer.ru*

*hxxp://sharksplayer2.com*

*hxxp://sharksplayer3.ru*

*hxxp://sharksreader.ru*

*hxxp://tema-info.ru*

*hxxp://toppfilms.ru*

*hxxp://video-movies.com*

*hxxp://video.909.su*

*hxxp://videodomm.ru*

*hxxp://videozzy.com*

*hxxp://videozzzz.ru*

*hxxp://websharks.ru*

*hxxp://yasmotrju.ru*

888



**Malicious MD5s known to have phoned back to the same IP (94.242.214.133):**

MD5: 9ec8aef6dc0e3db8596ac54318847328

MD5: 895c38ec4fb1fbee47bfb3b6ee3a170b

MD5: c4d88b32b605500b7f86de5569a11e22

MD5: 49861fd4748dd57c192139e8bd5b71e3

MD5: 8b350f8a32ef4b28267995cf8f0ceae1

**Premium rate SMS numbers involved in the fraudulent scheme:**

7151; 9151; 2855; 3855; 3858; 2858; 8151; 7155; 7255;  
3190; 3200; 3170; 3006; 3150; 6150; 4124; 4481; 7781;

5014; 1151; 4125; 1141; 1131; 1350; 3354; 7122; 3353;  
7132; 3352; 8355; 8155; 8055; 7515; 1037; 1953; 3968;

5370; 1952; 3652; 5373; 9191; 1005; 7019; 7250; 1951;  
7015; 7099; 7030

889



**Once executed MD5:  
9ec8aef6dc0e3db8596ac54318847328 phones back to  
the following C &C servers, further**

## **exposing the malicious infrastructure:**

67.215.246.10:6881

82.221.103.244:6881

114.252.58.66:6407

89.136.77.86:45060

212.25.54.183:32822

107.191.223.72:22127

87.89.149.106:24874

82.247.154.128:47988

108.181.68.73:47342

82.74.179.126:52352

121.222.168.146:64043

217.121.30.46:34421

115.143.245.78:51548

110.15.205.16:51477

37.114.69.97:19079

890

85.229.206.243:55955

95.109.112.178:60018

95.68.195.182:44025

239.192.152.143:6771

109.187.54.101:13100

117.194.5.97:55535

95.29.112.178:59039

109.162.133.97:19459

83.205.112.178:11420

95.68.3.182:53450

175.115.103.140:52696

197.2.133.97:27334

84.55.8.7:10060

27.5.132.243:19962

123.109.176.178:36527

175.157.176.178:22906

188.187.147.247:14745

178.212.133.205:52416

145.255.1.250:41973

213.21.32.190:51413

93.73.165.31:61889

176.97.214.119:46605

185.51.127.134:16447

109.239.42.123:16845

77.232.158.215:40266

178.173.37.2:47126

62.84.24.219:47594

37.144.87.15:13448

5.251.28.179:39620

94.19.66.51:42894

94.51.242.89:35691

93.179.102.216:24458

212.106.62.201:44821

95.52.69.39:12249

46.118.64.45:44172

217.175.33.130:45244

185.8.126.226:32972

93.92.200.202:56664

94.214.220.37:35196

46.182.132.67:32103

46.188.123.131:11510

83.139.188.142:34549

188.232.124.16:27582

91.213.23.226:19751

95.32.142.28:55555

95.83.188.157:15714

95.128.244.10:59239

176.31.240.170:6882

79.109.88.241:6881

91.215.90.109:34600

891

62.198.229.165:6881

91.148.118.250:21558

81.82.210.40:6881

97.121.23.163:31801

78.186.155.62:6881

78.1.158.105:47475

79.160.62.185:9005

213.87.123.81:17790

178.150.154.26:26816

83.174.247.71:59908

109.87.175.144:29374

86.57.186.171:45013



193.222.140.60:35691

176.115.158.138:24253

42.98.191.90:7085

178.127.152.72:10107

82.239.74.201:61137

185.19.22.192:46337

86.185.92.38:10819

78.214.194.145:24521

37.78.85.173:49001

82.70.112.150:32371

37.131.212.35:18525

79.136.156.151:59659

2.134.48.150:12530

95.29.164.86:6881

37.147.16.242:64954

79.45.36.86:22690

112.208.182.65:56374

62.99.29.74:44822

95.16.12.111:12765

124.169.69.69:41216

5.164.83.49:62348

79.22.73.216:61914

46.63.131.146:6881

89.150.119.203:55029

58.23.49.24:2717

83.41.5.241:45624

87.21.80.23:27949

178.150.176.150:57997

178.127.195.146:58278

5.141.236.13:15784

125.182.35.138:54094

99.228.23.82:29302

14.111.131.146:33433

122.177.90.137:25375

178.223.195.146:54596

182.54.112.150:1058

109.23.145.152:31514

213.241.204.31:27769

892

188.168.58.6:45823

2.94.4.215:50830

42.91.39.236:13923

116.33.113.4:19973

86.182.170.27:25712

177.82.206.231:39043

122.143.152.35:7890

217.13.219.147:39190

77.75.13.195:16279

87.239.5.144:58749

89.141.116.97:49001

176.106.11.49:44690

112.14.110.199:33243

122.26.6.52:20527

178.223.195.146:23034

98.118.85.85:51413

190.63.131.146:6881

46.151.242.82:16046

176.106.19.185:46114

85.113.157.12:62633

192.168.0.105:58749

211.89.227.34:56333

36.68.16.149:42839

31.15.80.10:42061

130.15.95.112:6881

87.119.245.51:6882

109.173.101.19:19700

193.93.187.234:1214

176.106.18.254:43469

176.183.137.53:19155

176.113.168.51:52672

93.123.60.130:52981

79.100.9.81:14053

91.124.125.16:29914

46.16.228.135:53473

95.61.55.234:22974

190.213.101.39:44376

58.173.158.99:50821

188.25.108.102:31047

95.153.175.173:15563

75.120.194.116:58001

61.6.218.126:63291

128.70.19.98:64296

5.167.193.5:25861

185.57.73.27:47892

109.205.249.105:58449

77.228.235.226:57715

2.62.49.161:49001

67.234.161.61:65228

91.243.100.237:40431

893

105.155.1.67:16084

73.34.178.71:41864

145.255.169.122:4612

92.241.241.4:61613

145.255.21.166:46596

83.253.71.148:34016

173.246.26.126:12988

79.181.115.213:43853

46.237.69.97:50772

86.159.67.146:48959

213.100.105.54:52147

178.45.129.126:45710

188.78.232.53:39336

70.82.20.41:11248

88.132.82.254:52722

85.198.154.126:35403

89.67.245.2:21705

95.76.128.209:36640

61.242.114.3:6383

79.112.156.169:10236

95.25.111.173:40781

108.36.82.254:57393

88.8.84.79:56740

118.36.49.220:59561

60.197.149.187:12996

86.26.224.104:39597

120.61.161.250:10023

151.249.239.173:6881

86.178.212.41:28489

95.180.244.144:48245

111.171.83.212:52952

122.164.99.166:1024

201.110.110.63:19314

79.100.52.144:54312

194.219.103.45:24008

178.89.171.19:10003

124.12.192.197:6881

92.96.186.112:31100

207.216.138.62:6881

194.8.234.230:51413

92.220.24.133:6881

2.134.203.233:6881

122.169.237.54:17407

36.232.153.137:16001

130.43.123.202:45689

86.73.45.54:56161

37.215.93.59:27997

78.154.164.176:42780

5.10.134.6:50452

98.176.222.50:61000

894

93.54.90.126:1189

220.81.46.201:51526

39.41.111.173:7702

41.111.41.122:19132

211.108.64.209:20728

178.66.212.41:14865

182.187.103.45:57751

118.41.230.79:52520

186.155.231.45:34294

109.174.113.128:15947

188.6.88.229:16785

99.247.58.79:23197

94.137.237.54:14617

197.203.129.67:10204

5.107.65.67:21618

117.194.114.71:64476

94.153.45.54:32715

2.176.158.50:17404

5.18.178.71:50971



78.130.212.41:63075

86.121.45.54:55858

109.187.1.67:15413

108.199.125.160:38558

83.181.18.121:15859

93.109.242.198:26736

95.86.220.68:27877

37.204.22.24:24146

198.203.28.43:17685

What's particularly interesting, about this campaign, is the fact, that, the Terms of Service (ToS) presented to

gullible and socially engineered end users, refers to a well known Web site (**jmobi.net**), directly connected with the market leading [11]**DIY API-enabled mobile malware generating/monetization platform**, extensively profiled in a

previously published post.

As cybercriminals continue to achieve a cybercrime-ecosystem wide [12]**standardization**, we'll continue to ob-

serve an increase in fraudulent activity, with the cybercriminals behind it, continuing to innovate, on their way to

achieve efficient monetization schemes, and risk-forwarding centered fraudulent models, further contributing to the

adaptive innovation to be applied to the current [13]**TTPs (tactics, techniques and procedures)** utilized by them.

1. <http://www.webroot.com/blog/2013/09/18/affiliate-network-mobile-malware-impersonates-google-play-tricks-users-installing-premium-rate-sms-sending-rogue-apps/>
  2. <http://www.webroot.com/blog/2013/10/08/newly-launched-vds-based-cybercrime-friendly-hosting-provider-help-s-facilitate-fraudulentmalicious-online-activity/>
  3. <http://ddanchev.blogspot.com/2013/08/profiling-novel-high-profit-margins.html>
  4. <http://ddanchev.blogspot.com/2013/11/fake-chromefirefoxinternet.html>
  5. <http://ddanchev.blogspot.com/2013/11/a-peek-inside-customer-ized-api-enabled.html>
  6. <http://ddanchev.blogspot.com/2013/09/rogue-iframe-injected-web-sites-lead-to.html>
  7. <http://ddanchev.blogspot.com/2013/08/dissecting-sample-russian-business.html>
  8. <https://www.virustotal.com/en/file/76b2e1a1b7c3079c782e8e1a6238fbf23c93bb3a3cf61a994fd872d478c492d7/analysis/1413910479/>
- 895
9. <https://www.virustotal.com/en/file/5ebdf263398fbd4d643c12>

[ea8cb8d1826862ad4b519bda95a09ed004bfc9c6cf/analysis/1413844185/](https://www.virustotal.com/en/file/ea8cb8d1826862ad4b519bda95a09ed004bfc9c6cf/analysis/1413844185/)

10.

<https://www.virustotal.com/en/file/d42aa42fd70f811b0f799f203b6d24ca003ee8cb83ab646de3e0eaa6e968616b/analysis/1413910495/>

11. <http://ddanchev.blogspot.com/2013/11/a-peek-inside-customer-ized-api-enabled.html>

12. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>

13. <http://www.webroot.com/blog/2013/12/27/cybercrime-trends-2013-year-review/>

896

# Document Outline

- 2013
  - January
    - [Historical OSINT: OPSEC-Aware Money Mule Recruiters Hire, Host Crimeware and Malvertisements \(2013-01-05 16:10\)](#)
    - [Historical OSINT - Profiling an OPSEC-Unaware Vendor of GSM/USB ATM Skimmers and Pinpads \(2013-01-05 20:42\)](#)
    - [Historical OSINT - Profiling an OPSEC-Unaware Vendor of GSM/USB ATM Skimmers and Pinpads \(2013-01-05 20:42\)](#)
    - [Raw Historical OSINT - Keeping Money Mule Recruiters on a Short Leash - Part Twelve \(2013-01-07 22:56\)](#)
    - [Raw Historical OSINT - Keeping Money Mule Recruiters on a Short Leash - Part Twelve \(2013-01-07 22:56\)](#)
    - [Summarizing Webroot's Threat Blog Posts for December \(2013-01-09 19:34\)](#)
  - February
    - [Summarizing ZDNet's Zero Day Posts for January \(2013-02-04 22:38\)](#)
    - [Summarizing Webroot's Threat Blog Posts for January \(2013-02-04 23:14\)](#)
    - [Historical OSINT - Hacked Databases Offered for Sale \(2013-02-06 02:03\)](#)
    - [Historical OSINT - Hacked Databases Offered for Sale \(2013-02-06 02:03\)](#)
    - [Dissecting NBC's Exploits and Malware Serving Web Site Compromise \(2013-02-21 22:03\)](#)

- [Dissecting NBC's Exploits and Malware Serving Web Site Compromise \(2013-02-21 22:03\)](#)
- [March](#)
  - [Summarizing Webroot's Threat Blog Posts for February \(2013-03-04 15:31\)](#)
  - [Dissecting NBC's Late Night with Jimmy Fallon Web Site Compromise \(2013-03-07 00:52\)](#)
  - [Dissecting NBC's Late Night with Jimmy Fallon Web Site Compromise \(2013-03-07 00:52\)](#)
- [April](#)
  - [Summarizing Webroot's Threat Blog Posts for March \(2013-04-01 21:37\)](#)
  - [Historical OSINT - The "BadB International" Cybercrime Enterprise \(2013-04-10 21:53\)](#)
  - [Historical OSINT - The "BadB International" Cybercrime Enterprise \(2013-04-10 21:53\)](#)
  - [What's the ROI on Going to a Virtual Blackhat SEO School? \(2013-04-17 23:45\)](#)
  - [What's the ROI on Going to a Virtual Blackhat SEO School? \(2013-04-17 23:45\)](#)
- [May](#)
  - [Summarizing Webroot's Threat Blog Posts for April \(2013-05-01 14:32\)](#)
  - [Fake 'Facebook Profile Spy Application' Campaign Spreading Across Facebook \(2013-05-24 18:58\)](#)
  - [Fake 'Facebook Profile Spy Application' Campaign Spreading Across Facebook \(2013-05-24 18:58\)](#)
  - [A Peek Inside the Russian Underground Market for Fake Documents/IDs/Passports \(2013-05-25 18:52\)](#)
  - [A Peek Inside the Russian Underground Market for Fake Documents/IDs/Passports \(2013-05-25 18:52\)](#)
- [June](#)

- [Summarizing Webroot's Threat Blog Posts for May \(2013-06-04 15:24\)](#)
- [Malware-Serving "Who's Viewed Your Facebook Profile" Campaign Spreading Across Facebook \(2013-06-10 15:07\)](#)
- [Malware-Serving "Who's Viewed Your Facebook Profile" Campaign Spreading Across Facebook \(2013-06-10 15:07\)](#)
- ['Anonymous' Group's DDoS Operation Titstorm \(2013-06-12 20:01\)](#)
- [Bogus "Shocking Video" Content at Scribd Exposes Malware Monetization Scheme Through Parked Domains \(2013-06-20 22:44\)](#)
- [Bogus "Shocking Video" Content at Scribd Exposes Malware Monetization Scheme Through Parked Domains \(2013-06-20 22:44\)](#)
- [Fake 'Rihanna & Chris Brown S3X Video' Spam Campaign Spreading Across Facebook, Monetized Through Adf Dot Ly PPC Links \(2013-06-22 10:56\)](#)
- [Fake 'Rihanna & Chris Brown S3X Video' Spam Campaign Spreading Across Facebook, Monetized Through Adf Dot Ly PPC Links \(2013-06-22 10:56\)](#)
- [July](#)
  - [Summarizing Webroot's Threat Blog Posts for June \(2013-07-04 18:38\)](#)
  - [Newly Launched 'Scanned Fake Passports/IDs/Credit Cards/Utility Bills' Service Randomizes and Generates Unique Fakes On The Fly \(2013-07-04 19:42\)](#)
  - [Newly Launched 'Scanned Fake Passports/IDs/Credit Cards/Utility Bills' Service Randomizes and Generates Unique Fakes On The Fly \(2013-07-04 19:42\)](#)

- [A Peek Inside a Managed OTP/ATS/TAN Token Bypassing/Hijacking/Blocking System as a \(Licensed\) Service \(2013-07-19 22:43\)](#)
- [A Peek Inside a Managed OTP/ATS/TAN Token Bypassing/Hijacking/Blocking System as a \(Licensed\) Service \(2013-07-19 22:43\)](#)
- [Instagram Under Fire as Cybercriminals Release New DIY Fake Account Registration/Management/Promotion Tool \(2013-07-23 17:01\)](#)
- [August](#)
  - [Summarizing Webroot's Threat Blog Posts for July \(2013-08-01 19:01\)](#)
  - [Dissecting a Sample Russian Business Network \(RBN\) Contract/Agreement Through the Prism of RBN's AbdAllah Franchise \(2013-08-10 21:10\)](#)
  - [Dissecting a Sample Russian Business Network \(RBN\) Contract/Agreement Through the Prism of RBN's AbdAllah Franchise \(2013-08-10 21:10\)](#)
  - [Spamvertised 'Confirmed Facebook Friend Request' Themed Emails Serve Client-Side Exploits \(2013-08-15 14:03\)](#)
  - [Spamvertised 'Confirmed Facebook Friend Request' Themed Emails Serve Client-Side Exploits \(2013-08-15 14:03\)](#)
  - [The Cost of Anonymizing a Cybercriminal's Internet Activities - Part Three \(2013-08-21 20:57\)](#)
  - [Vendor of Scanned Fake IDs, Credit Cards and Utility Bills Targets the French Market Segment \(2013-08-22 18:19\)](#)
  - [Vendor of Scanned Fake IDs, Credit Cards and Utility Bills Targets the French Market Segment \(2013-08-22 18:19\)](#)
  - [The Cost of Anonymizing a Cybercriminal's Internet Activities - Part Four \(2013-08-23](#)

17:16).

- Cybercriminals Offer High Quality Plastic U.S Driving Licenses/University ID Cards (2013-08-29 02:26).
- Cybercriminals Offer High Quality Plastic U.S Driving Licenses/University ID Cards (2013-08-29 02:26).
- Profiling a Novel, High Profit Margins Oriented, Legitimate Companies Brand-Jacking Money Mule Recruitment Scheme (2013-08-29 22:41).
- Profiling a Novel, High Profit Margins Oriented, Legitimate Companies Brand-Jacking Money Mule Recruitment Scheme (2013-08-29 22:41).
- Summarizing Webroot's Threat Blog Posts for August (2013-08-30 14:11).
- September
  - Rogue iFrame Injected Web Sites Lead to the AndroidOS/FakeInst/Trojan-SMS.J2ME.JiFake Mobile Malware (2013-09-16 14:29).
  - Rogue iFrame Injected Web Sites Lead to the AndroidOS/FakeInst/Trojan-SMS.J2ME.JiFake Mobile Malware (2013-09-16 14:29).
  - Dissecting FireEye's Career Web Site Compromise (2013-09-18 19:41).
  - Dissecting FireEye's Career Web Site Compromise (2013-09-18 19:41).
  - Spamvertised Facebook 'You have friend suggestions, friend requests and photo tags' Themed Emails Lead to Client-side Exploits and Malware (2013-09-28 13:53).
  - Spamvertised Facebook 'You have friend suggestions, friend requests and photo tags' Themed Emails Lead to Client-side Exploits and Malware (2013-09-28 13:53).
- October



- [Fake Pinterest 'Don't forget to confirm your email!' Themed Emails Serve Client-side Exploits and Malware \(2013-10-01 21:12\)](#)
- [Fake Pinterest 'Don't forget to confirm your email!' Themed Emails Serve Client-side Exploits and Malware \(2013-10-01 21:12\)](#)
- [Summarizing Webroot's Threat Blog Posts for September \(2013-10-02 16:10\)](#)
- [November](#)
  - [Summarizing Webroot's Threat Blog Posts for October \(2013-11-01 17:54\)](#)
  - [Malicious Script Artifacts at China Green Dot Gov Dot Cn - A Reminiscence of Asprox's Multi-Tasking Activities \(2013-11-04 18:33\)](#)
  - [Malicious Script Artifacts at China Green Dot Gov Dot Cn - A Reminiscence of Asprox's Multi-Tasking Activities \(2013-11-04 18:33\)](#)
  - [Scareware, Blackhat SEO, Spam and Google Groups Abuse, Courtesy of the Koobface Gang \(2013-11-04 18:36\)](#)
  - [Facebook FarmTown Malvertising Campaign Courtesy of the Koobface Gang \(2013-11-04 18:36\)](#)
  - [Money Mule Recruiters Trick Mules Into Installing Fake Transaction Certificates \(2013-11-04 18:37\)](#)
  - [A Peek Inside a Customer-ized API-enabled DIY Online Lab for Generating Multi-OS Mobile Malware \(2013-11-12 02:57\)](#)
  - [A Peek Inside a Customer-ized API-enabled DIY Online Lab for Generating Multi-OS Mobile Malware \(2013-11-12 02:57\)](#)
  - [New Commercially Available Modular Malware Platform Released On the Underground Marketplace \(2013-11-13 00:15\)](#)
  - [New Commercially Available Modular Malware Platform Released On the Underground](#)

[Marketplace \(2013-11-13 00:15\).](#)

- [Fake Chrome/Firefox/Internet Explorer/Safari Updates Expose Users to Android Malware \(2013-11-14 16:38\).](#)
- [Fake Chrome/Firefox/Internet Explorer/Safari Updates Expose Users to Android Malware \(2013-11-14 16:38\).](#)

○ [December](#)

- [Summarizing Webroot's Threat Blog Posts for November \(2013-12-03 23:38\).](#)
- [Facebook Circulating 'Who's Viewed Your Profile' Campaign Exposes 800k+ Users to CrossRider PUA/Rogue Firefox Add-ons/Android Adware AirPush \(2013-12-04 02:25\).](#)
- [Facebook Circulating 'Who's Viewed Your Profile' Campaign Exposes 800k+ Users to CrossRider PUA/Rogue Firefox Add-ons/Android Adware AirPush \(2013-12-04 02:25\).](#)
- [Continuing Facebook "Who's Viewed Your Profile" Campaign Affects Another 190k+ Users, Exposes Malicious Cybercrime Ecosystem \(2013-12-11 05:01\).](#)
- [Continuing Facebook "Who's Viewed Your Profile" Campaign Affects Another 190k+ Users, Exposes Malicious Cybercrime Ecosystem \(2013-12-11 05:01\).](#)

• [2014](#)

○ [January](#)

- [Summarizing Webroot's Threat Blog Posts for December \(2014-01-06 17:07\).](#)
- [Fake Adobe Flash Player Serving Campaign Utilizes Google Hosting/Redirection Infrastructure, Spreads Across Facebook \(2014-01-07 21:09\).](#)
- [Fake Adobe Flash Player Serving Campaign Utilizes Google Hosting/Redirection](#)

[Infrastructure, Spreads Across Facebook \(2014-01-07 21:09\)](#)

- [Dissecting the Ongoing Febipos/Carfekab Rogue Chrome/Firefox Extensions Dropping, Facebook Circulating Malicious Campaign \(2014-01-09 17:21\)](#)
- [Dissecting the Ongoing Febipos/Carfekab Rogue Chrome/Firefox Extensions Dropping, Facebook Circulating Malicious Campaign \(2014-01-09 17:21\)](#)
- [Facebook Spreading, Amazon AWS/Cloudflare/Google Docs Hosted Campaign, Serves P2P-Worm.Win32.Palevo \(2014-01-16 21:27\)](#)
- [Facebook Spreading, Amazon AWS/Cloudflare/Google Docs Hosted Campaign, Serves P2P-Worm.Win32.Palevo \(2014-01-16 21:27\)](#)
- [March](#)
  - [Summarizing Webroot's Threat Blog Posts for January \(2014-03-06 19:41\)](#)
  - [Summarizing Webroot's Threat Blog Posts for February \(2014-03-06 20:48\)](#)
  - [Win32.Nixofro Serving, Malicious Infrastructure, Exposes Fraudulent Facebook Social Media Service Provider \(2014-03-22 08:18\)](#)
- [October](#)
  - [Rogue Android Apps Hosting Web Site Exposes Malicious Infrastructure \(2014-10-21 21:24\)](#)